keybridge

Proposal to Administer a Environmental Sensing Capability

Response to DA 15-1426

GN Docket No. 15-319

Key Bridge LLC

Jesse Caulfield, CEO

1750 Tysons Blvd., Suite 1500
McLean, VA 22102

Phone: +1 (703) 542-4140

http://keybridgewireless.com

Document Information

Document Status	Public
Version	1.13.0
Date Printed	May 13, 2016
Copyright	© 2016 Key Bridge LLC. All Rights Reserved

Opening Letter

Key Bridge LLC (fmr Key Bridge Global LLC, dba "Key Bridge", "Key Bridge Wireless") is pleased to submit this proposal to administer a Environmental Sensing Capability in the 3.5 GHz frequency band.[1] This document responds to the Federal Communications Commission's Wireless Telecommunications Bureau and Office of Engineering and Technology invitation for proposal to operate a Spectrum Access System and to administer spectrum operations in the 3,550 to 3,700 MHz band (3.5 GHz).[2]

While this proposal makes reference to certain sections in our *Proposal to Administer a Spectrum Access System*, Key Bridge submits this proposal as an independent offer.

As in previous FCC initiatives Key Bridge has collaborated extensively through multi-stakeholder groups to help develop a body of industry standards and best practices to enable coexistence in 3.5 GHz. These standards are formative and still under development. Nevertheless we are committed and confident in our (and the community's) ability to develop and to implement transparent, neutral, inter-operable spectrum access and monitoring solutions for the 3.5 GHz band that meets or exceeds all of the Commission's requirements.

The Key Bridge ESC architecture and implementation is a comprehensive, end-to-end solution that completely satisfies or, where dependent upon incomplete standards or external factors, will be made to satisfy, all of the FCC's current requirements.. Our solution is also flexible enough to accommodate future changes or modifications to those requirements.

Key Bridge affirms that it will comply with all applicable rules and enforcement mechanisms and procedures in the operation of our ESC. Key Bridge also affirms that it will comply with subsequent guidance, clarifications and decisions as may be issued from time-to-time by the Commission concerning operation of a ESC. To the extent that Key Bridge may require to employ third party suppliers and/or service providers for any aspect of executing our duties Key Bridge will notify the Commission of such dependency and take care to ensure compliance is assured.

Key Bridge is happy to provide any additional information the Commission may require to evaluate this proposal.

/s/

Jesse Caulfield, CEO
Key Bridge LLC

[1] Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3700 MHz Band, GN Docket No. 12-354, *Report and Order and Second Further Notice of Proposed Rulemaking*, FCC 15-47 adopted April 17, 2015 (*Report and Order*)

[2] Public Notice, GN Docket 15-319 , *[WTB] and [OET] Establish Procedure and Deadline for … Applications*, DA 15-1426, Released 12/16/2015, (*Request for Proposal*)

Non-Conflict of Interest

The Key Bridge SAS will operate independently from the Key Bridge ESC.

Key Bridge intends to offer commercial ESC services to our own and to other FCC-designated and certified SAS administrator on a non-discriminatory basis. ESC services will be offered through a technologically neutral, standardized peering service.

Key Bridge hereby attests that our ESC services and information will be made available and offered to all subscribing SASs on a non-discriminatory basis.

Dependent Works

This document responds to Federal Communications Commission, Wireless Telecommunications Bureau and Office of Engineering and Technology invitation for proposal to operate a Spectrum Access System and to administer spectrum operations in the 3,550 to 3,700 MHz band as described in the Commissions 3.5 GHz *Report and Order*.

In its Report and Order the Commission invited interested parties to cooperatively develop and fine-tune various technical details of concepts and requirements introduced in its new Part 96 rules. These and other necessary aspects of Spectrum Access and Environmental Sensing have been taken up by multi-stakeholder groups whose work is ongoing and not complete.

Some sections of this proposal reference or are dependent upon these incomplete or planned works and must themselves necessarily be incomplete or lacking in detail.

Key Bridge will make best effort to implement relevant standards and recommendations produced by multi-stakeholder groups when those works are complete and available. We will amend or update affected sections of this proposal in future upon request.

Notices

This document is provided for the purpose of evaluating our candidacy to operate a Environmental Sensing System as envisioned in Part 96 of the Commission's rules. Many of the systems and methods presented herein are covered by issued or pending patents and other intellectual property rights and privileges.

NO GRANT OR PERMISSION IS PROVIDED OR IMPLIED TO ANY PROTECTED SYSTEM, METHOD, UTILITY, COPYRIGHT, TRADEMARK, ETC. BY ITS DISCLOSURE IN THIS PROPOSAL NOR MAY ANY RIGHT, GRANT OR PERMISSION BE PRESUMED OR ASSERTED AGAINST ANYTHING DISCLOSED HEREIN.

Table of Contents

Illustration Index

1 Responses to Compliance Requirements

Below we respond, directly and briefly, to the specific requirements identified in the Part 96 rules. Additional context and details are provided in this proposal.

Title 47: Telecommunication
PART 96—CITIZENS BROADBAND RADIO SERVICE
Subpart G—Environmental Sensing Capability

§96.67 Environmental sensing capability.

(a) The primary purpose of the ESC is to facilitate coexistence of Citizens Broadband Radio Service users with federal Incumbent Users through signal sensing. *An ESC will be operated by a non-governmental entity and, except as set forth in this section, will not rely on governmental agencies to affirmatively communicate information about the operations of incumbent radio systems.*	Reference Section 6 (Key Bridge ESC Concept of Operations) Key Bridge *ESC Infrastructure* is designed and will be deployed and operated to inform SAS peers of the availability (or unavailability) of spectrum according to a geographic partitioning strategy. Reference Section 4.2 (Business Structure) Key Bridge plus its partners and suppliers are non-governmental entities.
(b) An ESC may only operate after receiving approval by the Commission. *Such approval shall be conditioned on meeting the requirements of this part and any other requirements imposed by the Commission.* *The Commission may revoke, modify, or condition ESC approval at its discretion.*	An operational instance of the Key Bridge ESC Infrastructure described in this proposal will be proffered to the Commission for approval. Key Bridge understands and acknowledges that other government entities, including the NTIA, DoD, etc., may participate in and have a contributing or demurring role in such approval. Key Bridge further understands that such approval is not perpetual.
(c) An ESC must meet the following requirements:	
(1) Be managed and maintained by a non-governmental entity;	Reference Section 4.2 (Business Structure) Key Bridge and its partners and suppliers are non-governmental entities.
(2) Accurately detect the presence of a signal from a	Reference Section 6 (Key Bridge ESC Concept of Operations

federal system in the 3550-3700 MHz band and adjacent frequencies using approved methodologies that ensure that any CBSDs operating pursuant to ESC will not cause harmful interference to federal Incumbent Users;	The Key Bridge ESC will operate in a supporting role to a SAS. The ESC will determine the quality and quantity of interference protection afforded to federal incumbent users. The SAS retains responsibility to effect those protections. Reference Section 6.4 (Incumbent Sensing and Detection) Key Bridge is highly confident the ESC architecture, systems and methodologies described in this proposal will quickly and accurately detect the presence (or absence) of non-informing federal incumbent spectrum operations in the 3,550 to 3,700 MHz band and adjacent frequencies. Key Bridge proposes to develop, deploy, test and ultimately deploy one or a hybrid combination of methods to protect non-informing federal incumbent users in a phased approach, beginning with a conventional direct sensing strategy using fixed infrastructure and subsequently investigating other more sophisticated, cost effective and scalable solutions.
(3) Communicate information about the presence of a signal from a federal Incumbent User system to one or more approved SASs;	Reference Section 6.1 (SAS to ESC Peering) Key Bridge will employ a *SAS Gateway Protocol* to implement peering communications between SAS and ESC instances and to convey information about the presence (or absence) of federal incumbent users in a geographic region. The *SAS Gateway Protocol* is a proprietary, secure messaging protocol developed by Key Bridge. We intend to release the protocol as open-source software and to propose it as a standardized specification.
(4) Maintain security of detected and communicated signal information;	Reference Section 5.5 7 (Key Bridge ESC Security Architecture) Key Bridge *ESC Infrastructure* employs a layered security and positive communications model where data exchange is limited to designated applications and hosts.

	Access to information such as detected signal data is limited to the actual sensing apparatus and "neighboring" applications configured to process and analyze that data.
(5) Comply with all Commission rules and guidelines governing the construction, operation, and approval of ESCs;	Key Bridge and its partners and suppliers will comply with all Commission rules and guidelines governing approval, construction and operation of the Key Bridge *ESC Infrastructure*.
(6) Ensure that the ESC shall be available at all times to immediately respond to requests from authorized Commission personnel for any information collected or communicated by the ESC; and	Key Bridge will take care to ensure that the *ESC Infrastructure* will be available at all times to immediately respond to information requests by the Commission. Reference Section 5.5 (ESC Administration Portal) ESC Infrastructure is managed and administered through a *ESC Administration Portal*. The ESC Administration Portal incorporates several commercial-off-the-shelf applications to streamline configuration management plus health and status monitoring, accounting, fault management, performance management and security assurance.
(7) Ensure that the ESC operates without any connectivity to any military or other sensitive federal database or system and does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by this part to effectively operate the ESC.	Reference Section 5 (Key Bridge ESC High-Level Architecture) Key Bridge ESC Infrastructure does not rely upon government agencies for any information necessary to its function. Reference Section 6 (Key Bridge ESC Concept of Operations) The Key Bridge ESC does not *store* or *retain* spectrum sense data or information discerned from that data. Sense data is *transmitted* within the ESC between sensors and processing applications. These transmissions are positively protected in security enclaves using functional isolation and logical partition. The Key Bridge ESC solution does not *disclose* operational information on the position or movement

	of a detected incumbent user. Rather, the ESC translates and projects this information into geographically partitioned spectrum authorization instructions. It is conceivably possible for a maliciously observant SAS, with complete access to this information, to infer the presence of an incumbent user and to approximate its location within a local geographic region. Key Bridge believes however that a CBSD or network of CBSDs would be hard-pressed to make any such inferences. The Key Bridge solution incorporates several architectural features that serve to limit the geographic scope of unwanted information disclosure through unauthorized collection, misconfiguration or breach. Reference Section 7 (Key Bridge ESC Security Architecture) ESC Infrastructure solution enforces a *positive security model* to prevent unauthorized access, protect sensitive data and limit the effects of a potential breach, attach or failure. Other operational security aspects of ESC operation are the subject of continuing research in a multi-stakeholder group in which Key Bridge is a participant.[3] Key Bridge will take care to implement all relevant requirements, recommendations.
(d) ESC equipment may be deployed in the vicinity of the Exclusion Zones and Protection Zones to accurately detect federal Incumbent User transmissions.	Reference Section 6.2 (Logical Partitioning Strategy) *ESC Sensor Node* placement will be determined to achieve accurate, complete coverage of Exclusion Zones and Protection Zones.

[3] The Wireless Innovation Forum, Spectrum Sharing Committee, Working Group 2: *Security*.

2 Responses to Proposal Conformance Requirements

Below we respond, directly and briefly, to the specific requirements identified in the Commission's request for proposal. We also provide direct references to help the reader locate additional details in this proposal. Note that the direct references are indicative and not exclusive; they may be supplemented or supported by other aspects of the proposal and should be considered in the context of a end-to-end solution.

Wireless Telecommunications Bureau and Office of Engineering and Technology Establish Procedure and Deadline for Filing Spectrum Access System (SAS) Administrator(s) and Environmental Sensing Capability (ESC) Operator(s) Applications

GN Docket No. 15-319 , DA 15-1426 , Released: 12/16/2015

ESC Operator Requirements And Functions

All proposals must at a minimum include the following information:

1. A detailed description of the scope of the functions that the SAS and/or ESC would perform.	Reference Section 5 (Key Bridge ESC High-Level Architecture) The proposed ESC will implement all aspects of allowed and envisioned Part 96 operation.
2. A demonstration that the prospective SAS Administrator or ESC operator possesses sufficient technical expertise to operate an SAS and/or ESC, including the qualifications of key personnel who will be responsible for operating and maintaining the SAS and/or ESC.	Reference Section 4 (Key Bridge Qualifications) Key Bridge is technically capable to develop, test and receive certification and to operate the described *ESC Infrastructure* solution indefinitely. Key Bridge is the only TV-Bands spectrum administrator to have developed and operated a similar capability and integrated this capability into our TV-Bands white space database.
3. The prospective SAS Administrator or ESC operator must demonstrate that it is financially capable of operating an SAS and/or ESC for a five year term.	Reference Section 4.4 (Qualifications to Administer a ESC) Key Bridge is financially capable to develop, test and receive certification of the described ESC architecture and implementation. Key Bridge is also financially capable to operate a limited ESC sensor network indefinitely. We do not propose to operate a wide area sensor network as a speculative venture.
The proposal must include a	Reference Sections 4.2 (Business Structure) and 4.3

description of the prospective SAS Administrator or ESC operator's business structure including ownership information.	(Key Personnel) Key Bridge Wireless LLC (fmr "Key Bridge Global LLC" and dba "Key Bridge") is a limited liability corporation organized in the State of Virginia. Key Bridge is presently 100% owned by Mr. Jesse Caulfield, the sole managing partner.
To the extent that the proponent will rely on fees to support its operations, the proposal should also describe the fee collection process and the entities from which the fees will be collected.	Reference Sections 8 (Key Bridge ESC Commercialization Strategies) The 3.5 GHz ecosystem is emergent and rapidly evolving, as are various underlying commercialization strategies for fee recovery. Key Bridge may pursue several different commercialization strategies, each having its own fee collection process.
4. A description of how data will be securely communicated between the SAS and its associated ESC and how quickly and reliably these communications will be accomplished.	Reference Section 6.1 (SAS to ESC Peering) SAS – ESC peering is a message based open communications link. All transmissions are sender initiated (i.e. they follow a "PUSH" strategy) and messages are conveyed *immediately* to the receiver without delay. Reference Section 7.2 (Communications Security) Message reliability and information integrity is assured through the use of *WS-Security* authentication, integrity and confidentiality procedures.
5. Technical diagrams showing the architecture of the SAS and/or ESC and a detailed description of how each function operates and how each function interacts with the other functions.	Reference Sections 5 (Key Bridge ESC High-Level Architecture) and 6 (Key Bridge ESC Concept of Operations) *ESC Infrastructure* is implemented as a distributed, tightly-coupled client-server architecture of sensors and servers, and is comprised of a plurality *ESC Service Nodes* each supporting a local population of *ESC Sensor Nodes* and/or *ESC Fusion Nodes*.
6. A description of the propagation model and any other assumptions that the prospective SAS Administrator or ESC operator proposes to use to model	Reference Section 6.9.3 (Modeling Signal Propagation) Key Bridge proposes to use the IEEE 1900.5.2

operations and facilitate coordination in the band.	strategy of a modeled path loss to provide mathematically robust, repeatable CBSD coexistence and frequency coordination calculations without external dependency on a digital terrain model.
7. A description of the methods that will be used to update software and firmware and to expeditiously identify and address security vulnerabilities.	Reference Section 7.3 (Software Security) All software will be digitally signed. All applications will be configured with appropriate security permissions.
8. An affirmation that the prospective SAS Administrator and/or ESC operator (and its respective SAS and/or ESC) will comply with all of the applicable rules as well as applicable enforcement mechanisms and procedures.	Reference Opening Letter. Key Bridge affirms that it will comply with all applicable rules and enforcement mechanisms and procedures in the operation of our ESC. Key Bridge also affirms that it will comply with subsequent guidance, clarifications and decisions as may be issued from time-to-time by the Commission concerning operation of a ESC.

ESC proposals must also include the following information:

1. A description of the methods (e.g., interfaces, protocols) that will be used by the ESC to communicate with the SAS. *It must include a description of the security methods or protocols that will be used to ensure that unauthorized parties cannot access or alter the ESC or otherwise corrupt the operation of the ESC in performing its intended functions.*	Reference Section 6.1 (SAS to ESC Peering) SAS – ESC peering is a message based open communications link using a *SAS Gateway Protocol*. All transmissions are sender initiated (i.e. they follow a “PUSH” strategy) and messages are conveyed *immediately* to the receiver without delay. The *SAS Gateway Protocol* is a proprietary, secure messaging protocol developed by Key Bridge. We intend to release the protocol as open-source software and to propose it as a standardized specification. Reference Section 7.2 (Communications Security) All information exchanged between ESC and SAS is protected using a standards compliant implementation of *Web Services Security* (WS-Security) to enable secure communications across the Internet. Information is protected at the message level.
2. A description of the sensing methodology it will use to detect	Reference Section 6.4 (Incumbent Sensing and Detection)

federal transmissions and determine that the spectrum needs to be evacuated.	Initial operation of ESC Infrastructure will implement *direct incumbent sensing and detection* according to a conventional spectrum monitoring and signal classification strategy. Key Bridge proposes to conduct a independent and parallel development process to evaluate the efficacy of a *cooperative spectrum sensing and detection* strategy. If successful this alternate methodology will be independently proffered for certification. Reference Section 6.6 (Indirect Sensing Methodology) Key Bridge proposes to conduct a (second) parallel, independent development process to evaluate the efficacy of a "negative correlation" sensing methodology. If successful this alternate sensing and protection strategy will be independently proffered for certification. Reference Section 6.9 (Modeling and Computing Spectrum Coexistence) Key Bridge proposes to establish spectrum availability or unavailability according to a geographic partitioning strategy plus IEEE 1900.5.2-based modeling of incumbent radar transmitters and non-incumbent CBSD receivers.
This description must include a detailed description of the type of sensors to be used (i.e., infrastructure or device based), the sensing architecture to be employed, the sensing thresholds, any processing of sensor data, sensor sensitivity, and sensor resiliency to receiver front-end saturation and burn-out.	Reference Section 5.3 (ESC Service Node) Key Bridge proposes to employ a hybrid sensing strategy that includes both dedicated listening apparatus and device based cooperative spectrum sensing methodologies. ESC Infrastructure will consist of: • *ESC Sensor Nodes* for direct sensing • *ESC Fusion Nodes* for cooperative sensing • *ESC Service Nodes* for sensing data analysis *ESC Sensor Nodes* are dedicated listening devices supporting an infrastructure-based solution. *ESC Fusion Nodes* are processing applications that support a device-based sensing solution.

	ESC Service Nodes are data collection and analysis applications the implement ESC protection functionality and services for subscribing SASs. Key Bridge expects to refine implementation details of both methodologies (*direct* using Sensor nodes and *collaborative* using Fusion nodes) in consultation and collaboration with the Commission, NTIA and DoD during system review, testing and approval processes. Reference Section 6.4 (Incumbent Sensing and Detection) ESC Sensor Node hardware and software is still under development. These dedicated listening devices will meet or exceed all required performance specifications for sensor sensitivity and resiliency to receiver front-end saturation and burn-out. Key Bridge can provide the Commission with interim and/or final device performance specifications. The RF sensitivities of any deployed apparatus will be designed to accept, at minimum, the emissions of a RSEC Criteria C radar with AN/SPN-43 parameters.
The prospective ESC operator must also provide a description of the safeguards that will be used to "ensure that the ESC does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required to effectively operate the ESC by Part 96."	Reference Section 7 (Key Bridge ESC Security Architecture) The Key Bridge ESC does not *store* or *retain* spectrum sense data or information discerned from that data. Sense data is *transmitted* within the ESC between sensors and processing applications. These transmissions are positively protected in security enclaves using functional isolation and logical partition. The Key Bridge ESC solution does not *disclose* operational information on the position or movement of a detected incumbent user. Rather, the ESC translates and projects this information into geographically partitioned protection instructions. All ESC communications are cryptographically protected. ESC operational security aspects are the subject of continuing research in a multi-stakeholder group in

	which Key Bridge is a participant.[4] Key Bridge will take care to implement all relevant requirements, recommendations and best practices resulting from this work.
3. A description of the methods (e.g., interfaces, protocols) that will be used by sensors to communicate with the ESC and the procedures, if any, that it plans to use to verify that all sensors can communicate with the ESC in a timely and secure manner.	Reference Section 5 (Key Bridge ESC High-Level Architecture) *ESC Sensor Nodes* are directly administered and organized by a *ESC Service Node* and are cryptographically paired using digital keys and X.509 certificates. ESC Sensor Nodes are provisioned to respond to digitally signed status and performance queries from a Administration Portal. Reference Section 6.2 (Logical Partitioning Strategy) ESC Sensor Nodes are provisioned to send spectrum sense data to their designated ESC Service Node. ESC Sensor Nodes are provisioned, administered and monitored by an Administration Portal. This mutually authenticated relationship is cryptographically established and secured using digital keys and X.509 certificates.
It must include a description of the security methods or protocols that will be used to ensure that unauthorized parties cannot access or alter the ESC or individual sensors or otherwise corrupt the operation of the ESC in performing its intended functions.	Reference Section 7 (Key Bridge ESC Security Architecture) ESC Infrastructure is partitioned into security enclaves according to function and logical distinction. All data exchange is cryptographically protected using transport layer and message layer security, which includes standards compliant implementations HTTPS and of *WS-Security*.

[4] The Wireless Innovation Forum, Spectrum Sharing Committee, Working Group 2: *Security*.

3 Definitions and Abbreviations

This document incorporates by reference the various definitions relevant to operations in the 3.5 GHz band as provided by the FCC in 47 CFR 96.3. In addition, the following abbreviations are commonly used throughout this document.

ACS	Auto Configuration Server
API	Application Programming Interface
CBRS	Citizens Broadband Radio Service
CBSD	Citizens Broadband Radio Service Device; a type of CRS
CR-WSN	Cognitive Radio Wireless Sensor Network
CRS	Cognitive Radio System
DoD	U.S. Department of Defense
ESC	Environmental Sensing Capability
FCC	Federal Communications Commission
GA	General Authorized (typically when referring to a user)
GAA	General Authorized Access
IU	(Informing) Incumbent User; information is known *a priori*
LTE	Long-Term Evolution, marketed as 4G wireless service
NIIU	Non-Informing Incumbent User; information must be learned
NTIA	National Telecommunications and Information Administration
PA	Priority Access (typically when referring to a user)
PAL	Priority Access License
RF	Radio Frequency
SAS	Spectrum Access System

Table 1: Commonly used abbreviations.

4 Key Bridge Qualifications

Established in 2001, Key Bridge Wireless LLC is a privately held Virginia small business providing spectrum administration, spectrum monitoring, professional services and online information services to the Telecommunications industry, the U.S. Government, and the U.S. Military.

Illustration 1: Summary of Key Bridge capabilities

Key Bridge offers a broad portfolio of turn-key information services, data processing and analysis engines, as highlighted in Illustration 1.

Since 2013 Key Bridge has provided flexible dynamic spectrum access services in the VHF + UHF television bands, ensuring the safety and uninterrupted delivery for billions of dollars in over-the-air entertainment, sports and news media services. Key Bridge is a leading TV band white space administrator and the Key Bridge White Space Database & Portal is the preferred solution for spectrum users to ensure uninterrupted wireless services. Our portals, spectrum data and database services support a diverse population of spectrum users in a trusted, neutral manner.

In addition to spectrum administration services Key Bridge also offers managed spectrum monitoring solutions based upon our custom designed embedded intelligent spectrum sensors. Key Bridge spectrum sensors may be deployed and connected over any standard TCP/IP network and provide high performance remote signal monitoring and real-time carrier detection.

4.1 The Key Bridge Team

Similar to our approach for the VHF + UHF frequency bands, Key Bridge has assembled a team of industry leading companies to provide a complete portfolio of technology, infrastructure, resources, expertise and personnel needed to develop, deploy and maintain a state-of-the-art SAS + ESC solution.

Key Bridge support operations will be contracted similar to our TV-Bands white space database support operations. The Key Bridge support team provides a robust and fully staffed operations center with established operating procedures, methods and practices that yield average service availabilities above 99.9%.

Illustration 2: Key Bridge SAS / ESC operations center.

Key Bridge continues to work with Oracle as our preferred supplier of commercial hardware and software technology. Oracle is one of the world's largest contributors of open source technology and also the owner and provider of the Java Developer Kit (JDK) and Runtime (JRE), Java Enterprise Edition (J2EE), Java Micro Edition (J2ME), and Java Card technologies.

For flexible compute, collocation and connectivity resources Key Bridge employs Amazon’s cloud compute capabilities, which are supported by our own physical infrastructure co-located within Equinix facilities. Key Bridge and Cognitive Systems Corp. are working to perfect advanced, high-performance spectrum sensing technologies for the 3.5 GHz band. Earth Networks, our partner for distributed sensor network operations and management, presently operates the world's largest remote sensor network. Trace Systems, our partner for Federal and Military opportunities, provides assistance and coordination for Key Bridge ESC information security and operations security, and is our designated liaison for sensitive information exchange.

Oracle For almost 30 years, Oracle has helped customers manage their business systems and information with reliable, secure, and integrated technologies. Today, Oracle is the largest business software company in the world, with 345,000 customers - including 100 of the Fortune Global 100—and supports these customers in more than 145 countries.

Cognitive Systems Cognitive Systems Corp. develops high performance, reconfigurable wireless sensors and systems. CSC has extensive experience and expertise in advanced microchip design, digital signal processing, wireless protocols, firmware, software, cryptography and network/cloud infrastructure. Founded in 2014, Cognitive Systems' cloud-based spectrum sensing and monitoring solution is already proven and in use by the Canadian Government.

Earth Networks Founded in 1992, Earth Networks provides individuals, schools, businesses and government agencies live weather conditions, reports, and early warnings through its WeatherBug® service. With over 10,000 weather tracking stations and more than 1,000 cameras primarily based at neighborhood schools and public safety facilities across the U.S., Earth Networks presently operates the world's largest remote sensor network.

Trace Systems Trace Systems provides cybersecurity, intelligence, communications, networking and information technology services, systems, and solutions to the United States Department of Defense, Intelligence Community and Department of Homeland Security. We support our customers wherever and whenever they require our services and solutions. Since our founding in 1999 Trace Systems has been addressing mission critical requirements for the Department of Defense (DOD) in nearly every corner of the globe.

4.2 Business Structure

Key Bridge LLC (fmr “Key Bridge Global LLC”, dba “Key Bridge”, “Key Bridge Wireless ”) is a limited liability corporation organized in the State of Virginia. Key Bridge is 100% owned by Mr. Jesse Caulfield, the sole managing partner.

4.3 Key Personnel

Jesse Caulfield is the founder and CEO of Key Bridge Wireless LLC.

Mr. Caulfield has wide-ranging technical and business experience in cable, wireless and satellite service delivery. Mr. Caulfield chairs several industry groups, some specifically working to develop multi-stakeholder standards and standardized implementation guidelines for the emerging 3.5 GHz commercial ecosystem. Jesse frequently speaks at industry conferences and seminars and is widely recognized in the wireless community for his vision, thought leadership and expertise of dynamic spectrum access technologies and regulatory policy. Mr. Caulfield holds a degree in (High-Energy) Physics from the University of California, Los Angeles.

Mr. Taj Manku is a co-founder, Chief Business Development Officer & EVP Silicon of Cognitive Systems Corp.

Mr. Manku brings extensive experience in technical and executive management in the wireless communications field with a background in wireless technology development and wireless service delivery. Taj has over 100 granted patents and various awards in technology and business for his involvement in Software Defined Radios. Taj holds a degree in (Quantum) Physics and has a Ph.D. in Electrical Engineering from the University of Waterloo.

4.4 Qualifications to Administer a ESC

The Key Bridge team is technically competent and financially capable to develop, test and receive certification and to operate a ESC system architecture and implementation. Key Bridge is also financially capable to operate a limited ESC sensor network indefinitely.

Key Bridge does not propose however, nor commit, to deploy or to operate an expansive 3.5 GHz ESC system as a *speculative venture*. Rather, Key Bridge intends to deploy and to operate operate ESC infrastructure and sensor coverage in geographic regions based upon market demand.

Key Bridge has experience developing, deploying and operating a distributed spectrum sensing capability. Beginning in 2009 and operating until 2013, Key Bridge developed, deployed and operated a demonstration spectrum monitoring sensor network across the Northern Virginia / Maryland / Washington, DC region in support of our white space spectrum administration service and other prospective commercial users.

For this first generation spectrum sensing and monitoring capability Key Bridge commissioned a custom, low-cost, spectrum analyzer device which we embedded with a ruggedized computer system to provide ESC-type remote sensor capabilities. This embedded sensor apparatus included:

- Direct USB and Ethernet LAN connectivity plus WAN connectivity through a local computer system
- Frequency range from 5 to 2,500 MHz
- Resolution bandwidth from 10 KHz to 1 MHz
- Frequency accuracy +/- 1 kHz
- RF Sensitivity greater than -85 dBm
- Amplitude accuracy +/- 1 dB

In addition to the customized sensor hardware, Key Bridge also developed our own device driver and spectrum analysis software. We then integrated the custom spectrum sensor device with our software to create a complete remote spectrum analyzer system.

The Key Bridge remote spectrum sensor implemented, and the four-year Washington D.C. field operation demonstrated, many of the functions and capabilities called for in a 3.5 GHz spectrum band ESC. The Key Bridge system demonstrated detection, classification and geographic location of licensed (i.e. incumbent) services plus unlicensed or unrecognized services. The system collected and forwarded event and alarm information to a central repository for additional processing and analysis. The system was also able to stream raw sensor data for centralized comparative analysis.

Product information is included as an appendix to this proposal for reference. A presentation slide for a early network field trial conducted in Washington, DC is shown in Illustration 3.

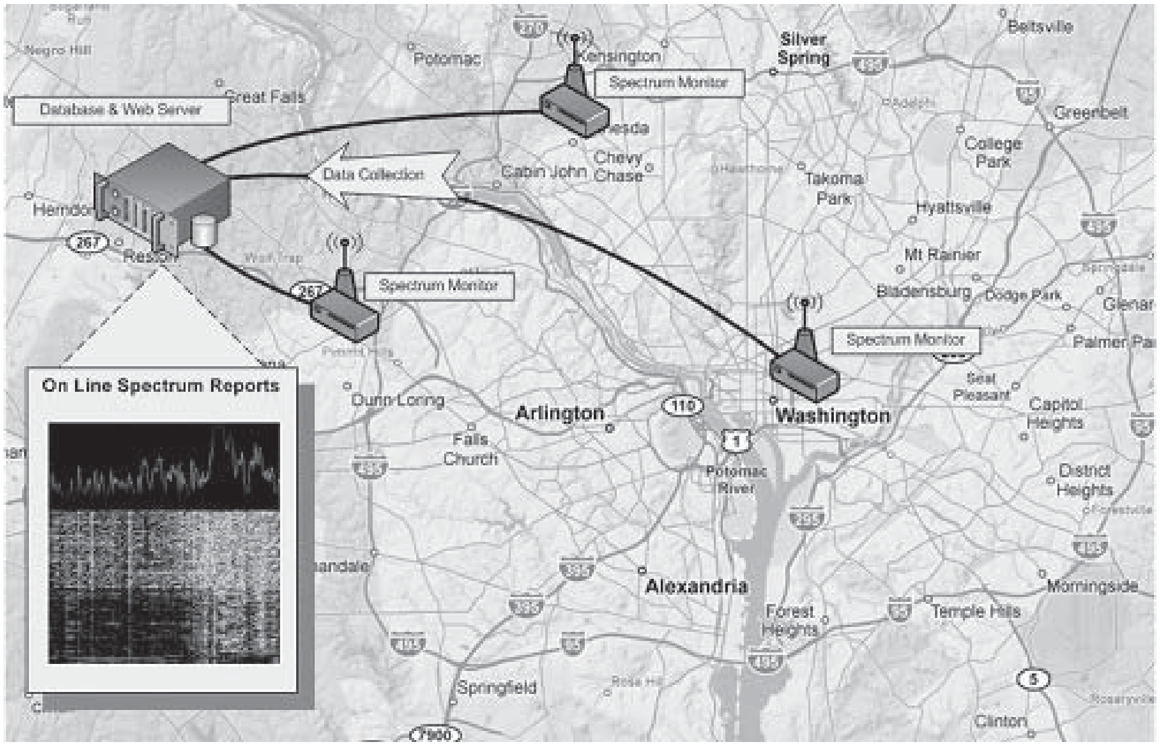


Illustration 3: Key Bridge demonstration sensor network (5-2,500 MHz)

For spectrum monitoring operations in the 3.5 GHz band Key Bridge proposes to build upon this demonstrated capability and expertise to develop, deploy and to operate a *second generation* remote spectrum monitoring and signal detection sensor network with strengthened security, improved interoperability, greater range and sensitivity plus more sophisticated data processing and analysis capabilities.

Key Bridge is committed to developing and implementing a transparent, inter-operable and secure spectrum monitoring and signal detection capability that meets or exceeds all of the Commission's requirements and incumbent concerns. We are not alone in this effort: Key Bridge recently organized and presently chairs a newly formed multi-stakeholder group to develop standards and best practices for multi-band, distributed spectrum sensor networks.

Key Bridge is competent and will take care to comply with all Commission rules, guidance and decisions related to a ESC. Key Bridge is technically and financially qualified to operate a ESC in compliance with Commission rules.

5 Key Bridge ESC High-Level Architecture

In its 3.5 GHz Report and Order the Commission offered the normative concept architecture for a spectrum sharing configuration shown in Illustration 4 that includes two primary systems: a *Spectrum Access System* (SAS), whose responsibility is to manage licensed and unlicensed users, and a *Environmental Sensing Capability* (ESC), whose responsibility is to detect non-informing incumbent users.[5] While not shown in the illustration is it commonly understood that there may exist multiple independent ESC implementations.

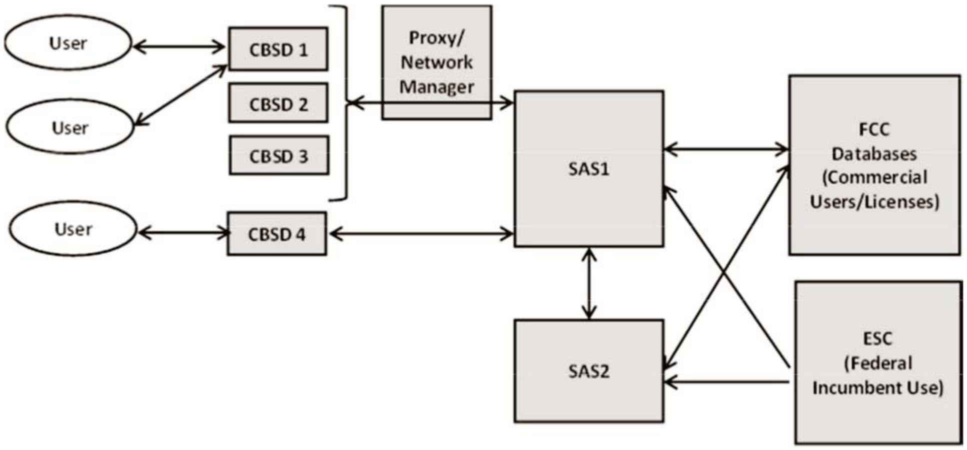


Illustration 4: Concept Citizens Broadband Radio Service architecture

3.5 GHz Citizens Broadband Radio Service Device (CBSD) operation is generally prohibited within various Exclusion Zones which include United States coastal regions and various inland areas.[6] CBSD operation is however allowed within the Exclusion Zones conditioned upon the successful detection and avoidance of an incumbent federal system. NTIA recommends and FCC Part 96 Rules envision an Environmental Sensing Capability (ESC) as a “system that detects … the presence of … an Incumbent User...” to protect the spectrum operations of incumbent federal systems and thereby enable CBSD use throughout the entire United States, including within Exclusion Zones.[7]

To effectively coordinate Priority Access (PA) and General Authorized Access (GA) users in the 3.5 GHz band the SAS is responsible for authenticating and authorizing CBSDs in both tiers of service and ensuring that those CBSDs operate within permissible technical parameters. In essence, the SAS’s role as akin to frequency coordination but with a high degree of automation. A SAS's ability to perform automated frequency coordination is critically dependent upon accurate, local, timely information about spectrum availability (or un-availability), which is

[5] FCC *Report and Order*, Figure 3 at page 95.

[6] The National Telecommunications and Information Administration (NTIA) Letter to FCC on Commercial Operations in the 3550-3650 MHz Band, GN Docket No. 12-354, March 24, 2015 (*NTIA Letter*); Ground based Exclusion Zones and Shipborne Radar Envelope Coordinates at https://www.ntia.doc.gov/fcc-filing/2015/ntia-letter-fcc-commercial-operations-3550-3650-mhz-band

[7] 47 CFR 96.3 – Definitions

established by a ESC as the absence (or presence) of incumbent user activity.

The FCC-provided notional architecture in Illustration 4 may be readily extended to that shown in Illustration 5 by providing additional detail for how a SAS may receive information about *informing incumbent user* (IU) and *non-informing incumbent user* (NIIU) spectrum operations. Referring to the extended notional model in Illustration 5 the SAS learns about IU directly from a FCC data source and about NIIU from a ESC.

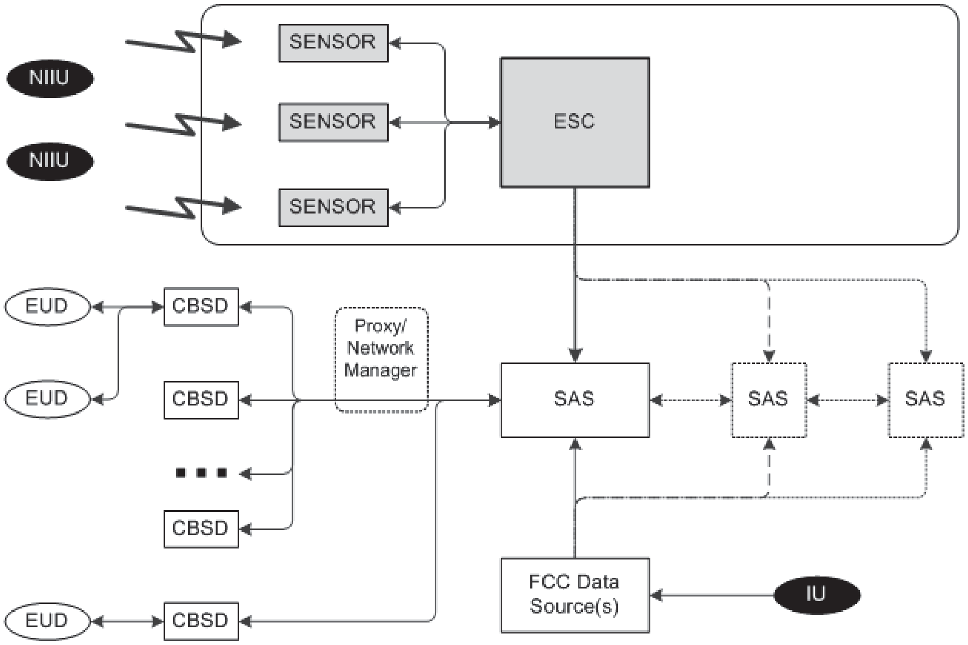


Illustration 5: FCC architecture extended to show IU and NIIU detection.

In this model the ESC's function is to discern the presence (or absence) of a signal from a non-informing incumbent user. Information about the the NIIU's presence, originating in the ESC, is required by the SAS to effect the protection of the NIIU's spectrum operation, which is implemented by selectively authorizing or de-authorizing CBSD operations (which are identified as Access Points (“AP”) in the diagram).

5.1 ESC Solution Overview

The Key Bridge environmental sensing capability solution is exactly that: a spectrum sensing *capability*. This capability will be implemented with custom software, integrated computer systems, plus commercial off-the-shelf sensor technologies and will employ a variety of spectrum sensing strategies to match particular user types and operating environments.

Our ESC solution is designed as a distributed, partitioned application with localized information scope and global device management, control and oversight. In its simplest form a Key Bridge ESC contains one or more *ESC Sensor Nodes*, plus several applications to administer the sensors and their data, which are geographically partitioned and managed by *ESC Service Nodes*. Collectively this “system of systems” establishes a complete environmental sensing *capability* and is called a *ESC Infrastructure*.

- **ESC Infrastructure** is the collection of *ESC Sensor Nodes* and associated *ESC Service Node* applications that collectively establish and provide a FCC Rules-compliant incumbent detection capability.
- **ESC Service Node** is a set of server applications that administer and manage the operations of various *ESC Sensor Nodes*.
- **ESC Sensor Node** is a spectrum signal and data processing system configured to detect and to classify radio signals.

5.2 ESC Infrastructure

Key Bridge *ESC Infrastructure* is a hierarchical sensor network with a root level Administration Server and other supporting applications that provide administration, management, oversight, plus run-time configurations and policy information to various ESC Service Nodes, which are the service providing entities within the ESC Infrastructure.

ESC Service Nodes are provisioned to provide authoritative ESC services for a geographic area or region. ESC Service Nodes provide this service through ESC Sensor Nodes, which they administer and manage. This hierarchical architecture is shown in Illustration 11, with administration functions on the left, sensing apparatus on the right, and service delivery applications in the center.

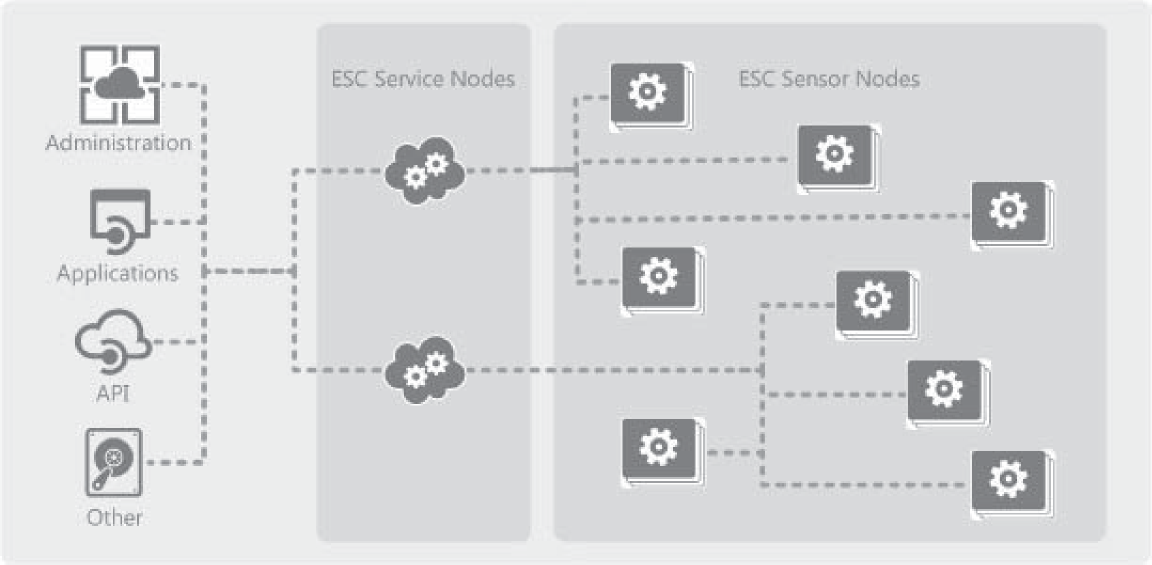


Illustration 6: ESC Infrastructure is organized hierarchically.

ESC Infrastructure data communications and message routing is configured according to a *directed acyclic graph* topology, where message exchange is strictly hierarchical and may only pass from one layer to the next. For example, referring again to Illustration 6, while several ESC Sensor Nodes may be provisioned on a common local area network those nodes are configured to only communicate with their *parent* ESC Service Node; inter-Sensor Node communication is disallowed by configuration.

Internally a Key Bridge *ESC Infrastructure* is implemented as a distributed, loosely-coupled client-server architecture of sensors and servers and is administered through a *ESC Administration Portal*. Radio frequency sensing is implemented by *ESC Sensor Nodes*, which are physically installed in a geographically distributed configuration. The various ESC Sensor Nodes are provisioned and configured to execute RF sensing, data processing and incumbent detection over a geographic region. Multiple *Service* and *Sensor Nodes* are deployed to establish a distributed spectrum sensor network and to achieve full RF sensing capability over an extended geographic area.

5.2.1 Administration Applications

Administration applications such as the ESC Administration Portal have *global scope*. That is: they may initiate a communication with, or establish a operating configuration for, components throughout the ESC Infrastructure.

- **Administration Portal** provides global system administration, management and oversight.
- **Administration Applications and API** support automated FCAPS model processes, which includes fault management, configuration management, accounting, performance management and security assurance.

5.2.2 Embedded Applications

Other applications run embedded within a ESC Service Node and have *local scope*. Locally scoped applications and may communicate only with other software applications in the same logical partition (i.e. enclave) or with applications identified as having global scope. The expected placement of these various applications in the ESC operating architecture is logically partitioned into *data*, *service* and *administration* security domains and is shown in Illustration 7, where the anticipated application relationship with other various ESC functional components is presented.

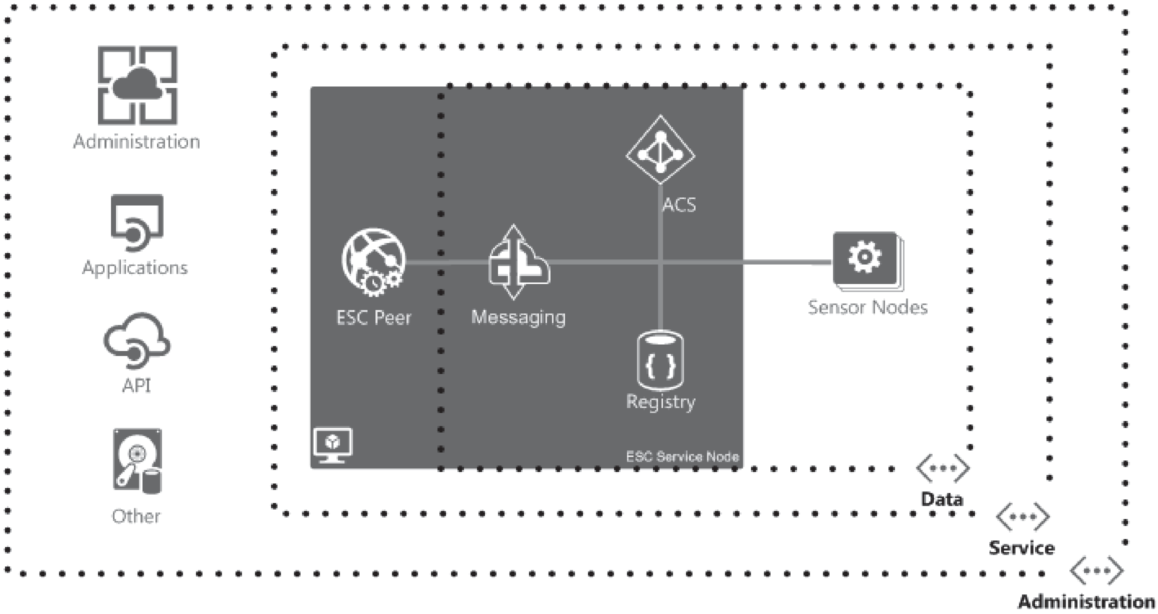


Illustration 7: ESC Infrastructure incorporates layered security domains.

Reference section 7 (Key Bridge ESC Security Architecture) for additional information about enclaves and their use in establishing and maintaining security domains.

- **Auto Configuration Server** (ACS) provides provides automatic ESC Node configuration and policy distribution. The ESC Auto Configuration Server (ACS) is a vendor-agnostic, end-to-end service fulfillment and device provisioning solution to manage and monitor remote ESC Sensor Nodes over any network.
- **Registry** contains a database repository of ESC Nodes and their available spectrum sensing capabilities, including service coverage areas.
- **Messaging Provider** allows secure, asynchronous messaging exchange from ESC Nodes to subscribed client SAS Nodes.

The peering application in a ESC Service Node has a special scoped configuration and acts as a communications gateway, allowing managed data communications between the ESC Messaging Provider and *positively* identified external systems, such as a SAS. Reference section 7 (Key Bridge ESC Security Architecture) for additional discussion about positive security model implementation.

- **Peering Gateway** provides a standardized external interface for automated access and machine-to-machine services.

5.2.3 Other Applications

Other applications in the ESC Infrastructure are still under review and their placement and organization within the architecture is not yet determined. For example, the following applications still “need a home”. Several of the applications listed require access to raw sensor data, which is expensive to transport over long distances, and will probably “live” close to the spectrum sensors. This is balanced with their requirement for high-power computation and also their cost of licensing.

- **Vector Signal Analysis** (VSA) software is an industry standard used throughout the wireless communications and aerospace/defense industries for collection and processing of all forms of RF signals.
- **Transmitter Location** may be a required capability for the indirect incumbent spectrum sensing strategy described in section 6.6 (Indirect Sensing Methodology). Transmitter location provides geolocation measurements on signals of interest using either time or power based triggering using Time Difference of Arrival (TDOA), Received Signal Strength (RSS) or a hybrid adaptive algorithm that uses both time and power information.
- **A Developer API** may be added to support to support other spectrum uses that require spectrum monitoring capability but that are not related to CBRS operations. For these applications a method is needed to task ESC Sensor Nodes and to receive spectrum sense data independent from CBRS requirements.

5.3 ESC Service Node

ESC Service Nodes are the the service providing components in the ESC Infrastructure. That is: A SAS receives ESC information services provided by a ESC Service Node.

ESC services provided by a ESC Service Node to a SAS are valid only within a specific geographic region within which the ESC has NIIU detection capability. Each ESC Service Node *geographic partition* is called a ESC Service Area.

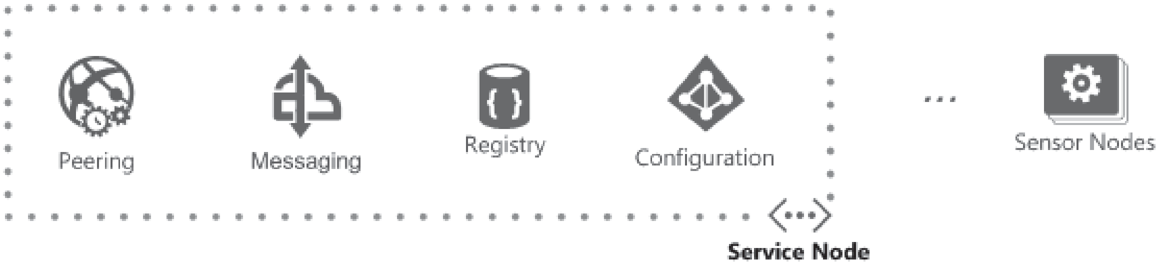


Illustration 8: ESC Service Node includes local application instances.

ESC Service Nodes are logically partitioned by running discrete, possibly virtualized, instances of the various server applications required to operate and manage a set of ESC Sensor Nodes. These application partitions generally comprise a *peering*, *messaging*, *registry* and *configuration* server application. This organizing principle is shown in Illustration 8.

5.4 ESC Sensor Node

A *ESC Node* is a generic spectrum signal and data processing application configured to detect, discern and classify radio signals. A ESC Node may include an embedded spectrum sensor or it may receive spectrum data from one or more external sensor devices. There are two basic categories of ESC Node envisioned in a Key Bridge ESC Infrastructure: a *Sensor Node* and a *Sensor Fusion Node*.

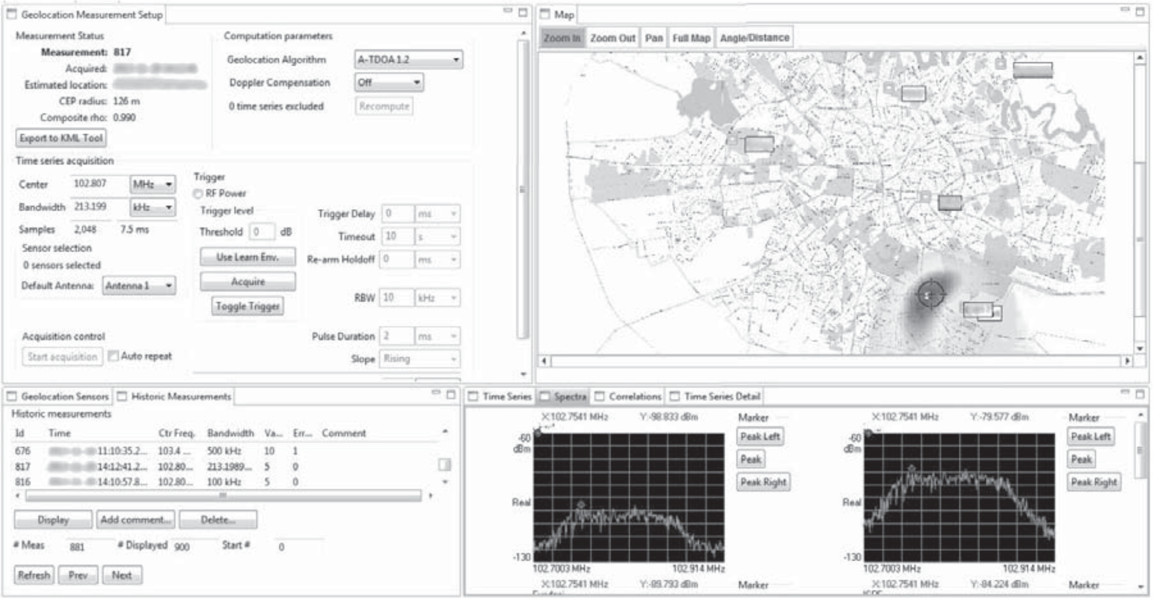
- **Sensor Node** is a embedded computer apparatus that *contains a radio listening device* and also *contains embedded spectrum signal processing capabilities*. Examples include a conventional spectrum analyzer, a spectrum monitor and software defined radio having embedded spectrum and signal processing capability.
- **Sensor Fusion Node** is a embedded computer apparatus that *does not contain a radio listening device* but does contain embedded spectrum signal processing capabilities. A Sensor Fusion Node receives input spectrum data from external collection sources.

ESC Sensor Nodes and Sensor Fusion Nodes implement different methods of data collection and analysis. Both node types provide sensing *capability.* ESC Sensor Nodes and Sensor Fusion Nodes both support a ESC Service Node and (in theory) are not discernible from the perspective of a subscribing client.

Key Bridge has high confidence in the direct sensing strategy using Sensor Nodes, and we hope to prove (or disprove) the efficacy of Sensor Fusion Nodes during the ESC development, testing and certification process.

5.5 ESC Administration Portal

ESC Infrastructure is managed and administered through a *ESC Administration Portal* that will build upon and incorporate the sensor network management technologies, processes and experiences from our earlier sensor network deployments. The Key Bridge ESC Administration Portal will also incorporate several commercial-off-the-shelf applications to streamline configuration management plus health and status monitoring, accounting, fault management, performance management and security assurance.



Geolocation Measurement Setup

Measurement Status

Measurement: 817
Acquired: [redacted]
Estimated location: [redacted]
CEP radius: 126 m
Composite rho: 0.990

Computation parameters

Geolocation Algorithm: A-TDOA 1.2
Doppler Compensation: Off
0 time series excluded

Time series acquisition

Center: 102.807 MHz
Bandwidth: 213.199 kHz
Samples: 2,048 7.5 ms
Sensor selection
0 sensors selected
Default Antenna: Antenna 1

Trigger
○ RF Power
Trigger level
Threshold: 0 dB
Trigger Delay: 0 ms
Timeout: 10 s
Re-arm Holdoff: 0 ms
RBW: 10 kHz
Pulse Duration: 2 ms
Slope: Rising

Acquisition control
□ Auto repeat

Historic measurements

Id	Time	Ctr Freq.	Bandwidth	Va...	Err...	Comment
676	[redacted] 11:10:35.2...	103.4 ...	500 kHz	10	1	
817	[redacted] 14:12:41.2...	102.80...	213.1989...	5	0	
816	[redacted] 14:10:57.8...	102.80...	100 kHz	5	0	

Meas 881 # Displayed 900 Start # 0

X:102.7541 MHz Y:-98.833 dBm
X:102.7541 MHz Y:-79.577 dBm
X:102.7541 MHz Y:-89.793 dBm
X:102.7541 MHz Y:-84.224 dBm

Illustration 9: Example of a ESC Administration Portal application.

In addition to sensor network management, the Administration Portal will also include a spectrum viewer application to perform ad-hoc inspection of the local spectrum environment. A sample screen shot of one sensor administration application presently under evaluation and demonstrating this capability is shown in Illustration 9.[8]

[8] Reproduced with Permission, Courtesy of Keysight Technologies, Inc.

6 Key Bridge ESC Concept of Operations

Note: ESC architectures, protection strategies, configurations and SAS to ESC communications protocols are still under development both internally by Key Bridge and also publicly in multi-stakeholder groups. The concepts described below reflect our current estimates for how a production ESC will be organized and operated. The actual, final configuration may differ in detail but we believe the organizing principles are sound.

Definition: For the rest of this document the term "Environmental Sensing Capability" and its abbreviation "ESC" are used alternatively with "ESC Infrastructure" as a spectrum sensor network operated by a single party; the term "ESC" is therefore not used as a generic *capability to detect* but rather as the actual system doing the detection.

FCC Part 96 Rules do not prescribe mechanisms or strategies by which a SAS, when operating with the support of a ESC, may conditionally allow a CBSD to operate within an exclusion zone.[9] Instead the Rules require that CBSD operations not cause harmful interference to federal incumbent users where allowed by a ESC.[10] Implementation of this requirement is the responsibility of a SAS, whose job is complicated by the large number of expected CBSD devices. A relatively simple strategy for implementing NIIU interference protection in a SAS that may be quickly and easily applied to very large and potentially dense CBSD populations is therefore desired.

Part 96 Rules envision a ESC architecture composed of a distributed network of spectrum sensors but the Rules are also silent on exactly how a ESC should implement detection and at the same time not disclose sensitive information about NIIU spectrum operations.

NTIA and the FCC both envision that a ESC will "not be necessary everywhere, but only in the vicinity of the exclusion zones established to protect the federal radar systems (i.e., along the coasts for shipborne radars and near facilities used for ground-based radar operations)."[11]

The FCC envisions that a SAS and ESC will be independently evaluated and certified for operation. The proposed Key Bridge architecture formalizes this relationship by establishing separate and independent SAS and ESC operations with mechanisms for neutral, secure information flow between them, called *peering*.

[9] 47 CFR 96.15(a)(3). "Exclusion Zones shall be maintained along the Coastline …." Note that NTIA is responsible for establishing and maintaining Exclusion Zone definitions.

[10] 47 CFR 96.67(c)(2), "... ensure that any CBSDs operating pursuant to ESC will not cause harmful interference to federal Incumbent Users"

[11] NTIA Letter at 3.

6.1 SAS to ESC Peering

Key Bridge expects the FCC to authorize more than one party to operate a ESC, and that the internal architecture and configuration of each ESC may differ. Key Bridge further expects that each ESC, or at least the ESC in this proposal, will be independent and autonomous to the one or more SASs that depend upon their respective ESC for incumbent detection. The same principal applies in reverse as well: a SASs internal architecture and configuration is also independent and autonomous to its ESC, and each ESC may pursue different strategies and implement different technologies for incumbent detection.

Regardless of their respective internal architecture, technology and detection strategies, a ESC and SAS must interface to share information about spectrum availability or un-availability. This essential concept is called *peering* and is shown in Illustration 10. Through peering a SAS and ESC may may exchange data in a neutral manner irrespective of their internal architecture and configuration.

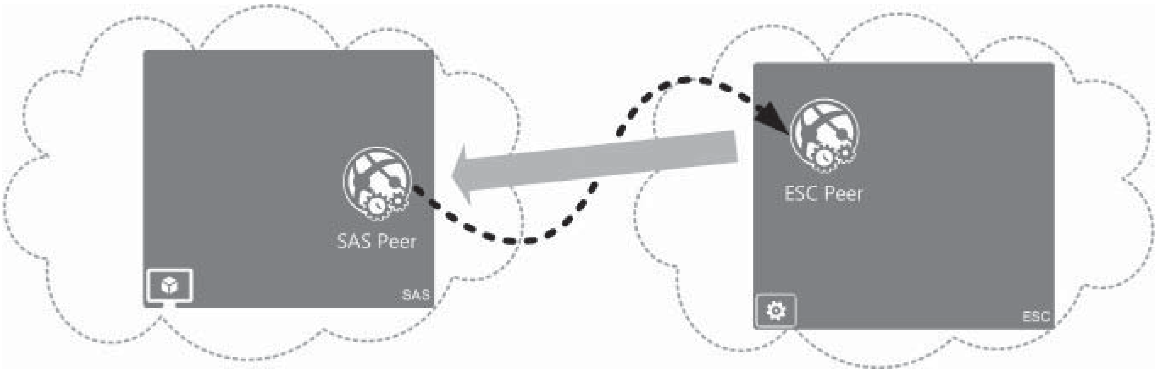


Illustration 10: SAS to ESC Peering masks internal architecture.

A SAS exterior peering protocol standard will place no constraint on the internal architecture and operation of the various entities that use the protocol. Referring again to Illustration 10, a generic peering process enables SAS of unknown constitution on the left peers with a Key Bridge ESC on the right.

SAS to ESC peering operational security policies and configurations are under development within a multi-stakeholder group in which Key Bridge is a participant.[12] The actual protocol and data structures for SAS to ESC peering is not the subject of multi-stakeholder group consideration. Key Bridge has therefore invented proprietary and also proposed non-proprietary methods that a SAS may use when coordinating with a ESC to dynamically protect a non-informing incumbent spectrum user. The Key Bridge *SAS Gateway Protocol* is, at present, a proprietary application peering protocol that includes mechanisms to support cryptographically secure message exchange for both SAS to SAS and SAS to ESC peering, including all security prescriptions identified by the multi-stakeholder group.

[12] The Wireless Innovation Forum, Spectrum Sharing Committee, Working Group 2: *Security*.

A SAS and ESC Peering relationship using to the *SAS Gateway Protocol* is secure and neutral. A SAS Infrastructure may register with and receive information from any inter-operable ESC Infrastructure supporting a peering service. When using the Key Bridge SAS Gateway Protocol a compatible SAS may register with and receive information from a compatible ESC via a designated *ESC Peering API*.

In the Key Bridge architecture ESC Service Nodes are responsible for NIIU detection services and peer directly with a subscribing SAS via the SAS Gateway Protocol. This strategy is designed to limit the geographic extent of NIIU information conveyed to a SAS to that necessary for the SAS to administer CBSDs in a specific geographic region. However, the ESC places no constraint on SAS internal architecture or operation, and a SAS may peer with multiple ESC Service Nodes.

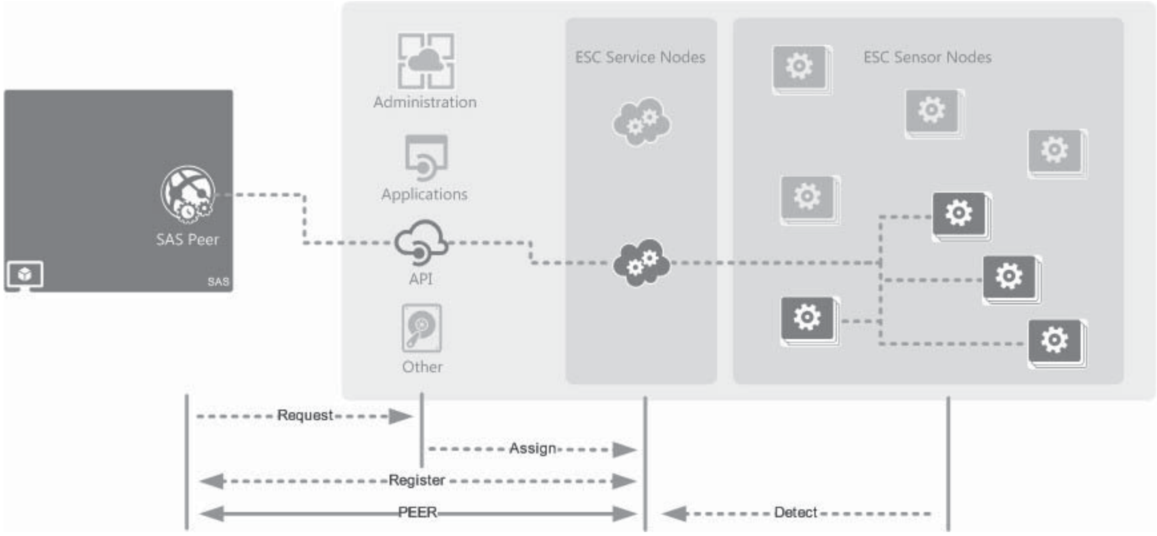


Illustration 11: ESC Service Nodes provide NIIU detection services to a SAS.

The process of a generic SAS peering with the Key Bridge ESC Infrastructure is detailed in Illustration 11, and proceeds according to the following general strategy.

- **Request**. A SAS first inquires about service availability to the ESC Infrastructure via a general peering API interface. The SAS service request includes the geographic area or areas where the SAS wishes to provide spectrum administration. If ESC services are not available in the requested geographic area the request is rejected (i.e. fails), otherwise the request is assigned to a matching ESC Service Node.
- **Assignment**. If NIIU detection capability is available in the SAS requested geographic area the ESC Infrastructure will assign the SAS registration request to a matching ESC Service Node.
- **Register**. After a geographic match has been established the respective ESC Service Node and the SAS exchange detailed information necessary to establish a direct and

persistent peering relationship. The registration process includes conveying to the ESC Peer the specific SAS geographic regions of responsibility plus instructions describing how the ESC may query the SAS for additional information and also how to notify the SAS of ESC spectrum availability information, updates and instructions.

- **Peer**. Once established the ESC Service Node will respond to spectrum availability requests within its geographic area of service and also inform the SAS about any changes in spectrum availability.

An artifact of this CONOPS is that the Key Bridge ESC Service Nodes are assigned responsibility to determine the quantity and quality of protection for the incumbent user within their ESC Service Area, while responsibility to effect that protection is retained within a SAS. That is to say: A *ESC Service Node* is the service providing component of the ESC Infrastructure, and it is the ESC Service Node that authorizes or de-authorizes CBSD operations within their responsible service area according to a *geographic partitioning strategy* within their respective ESC Service Area.

6.2 Logical Partitioning Strategy

All NIIU are actively protected in a SAS by default unless and until their absence is positively confirmed by a ESC, in accordance with Commission rules. The ESC, acting independently and autonomously to the SAS, notifies the SAS of the presence or absence of a federal NIIU.

ESC Sensor Nodes are deployed and configured to implement Rules-compliant spectrum sensing over a defined geographic region or ESC Sensor Node *coverage area*. A ESC Sensor Node coverage area is defined as the geographic region within which NIIU detection may be established with a high degree of confidence. The details and specific definitions of NIIU *detection* and *confidence of detection* are under study in a multi-stakeholder group in which Key Bridge is a member and participant.[13]

NIIU spectrum operations are detected by *ESC Sensor Nodes*, whose regions of effective sensor coverage may overlap. This concept may be explained by referring to Illustration 12, where three ESC Sensor Nodes and their corresponding coverage areas are shown. ESC Sensor Node configurations may also be locally optimized for that sensor's physical configuration and may implement various strategies such as, for example, tuning each sensor's receiving sensitivity, strategically locating sensor installations, employing directional antennae to shape the effective sensor coverage, etc.

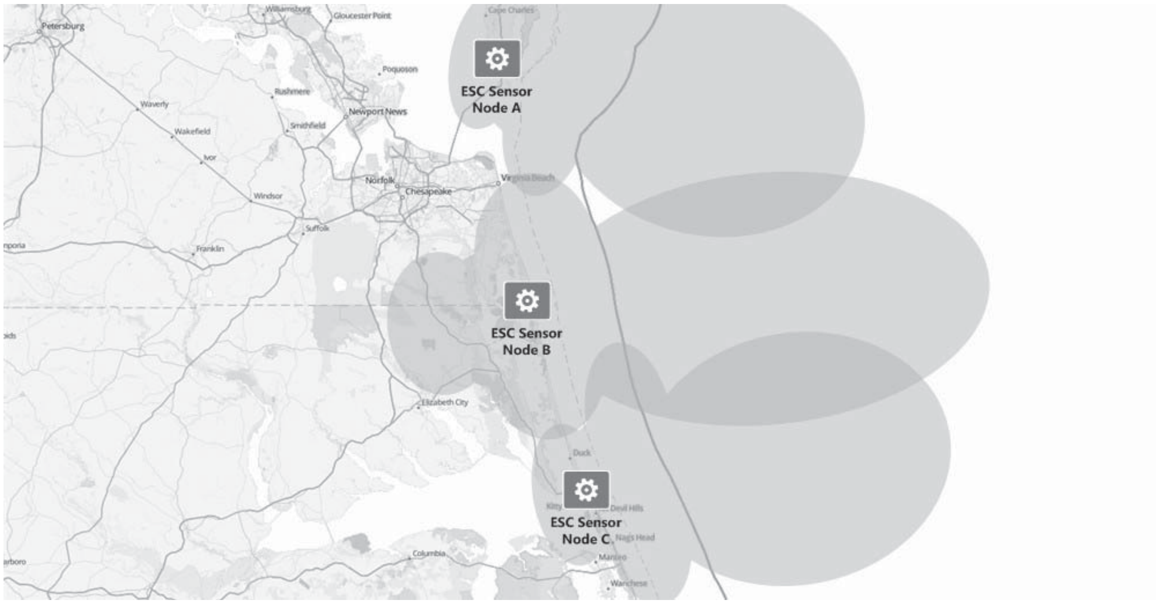


Illustration 12: Example coastal deployment with overlapping coverage areas.

In the illustrated example three ESC Sensor Nodes are installed along a coastal region such that each of their coverage areas (that is, their *effective sensor range*) overlap to create a continuous and uninterrupted detection capability.

[13] The Wireless Innovation Forum, Spectrum Sharing Committee, Working Group 1: *Requirements*

This regional detection capability provided by one or more ESC Sensor Nodes is then aggregated by ESC Service Node into a larger *ESC Service Area*. The ESC Service Area is the unit of geographic coverage externally represented to a SAS.

NIIU detection services are informed by the network of ESC Sensor Nodes that operate in that area under the ESC Service Node's management and coordination. An example instance showing the organization and management of multiple *ESC Sensor Nodes* by a *ESC Service Node*, and the corresponding establishment of a *ESC Service Area*, is provided in Illustration 13.

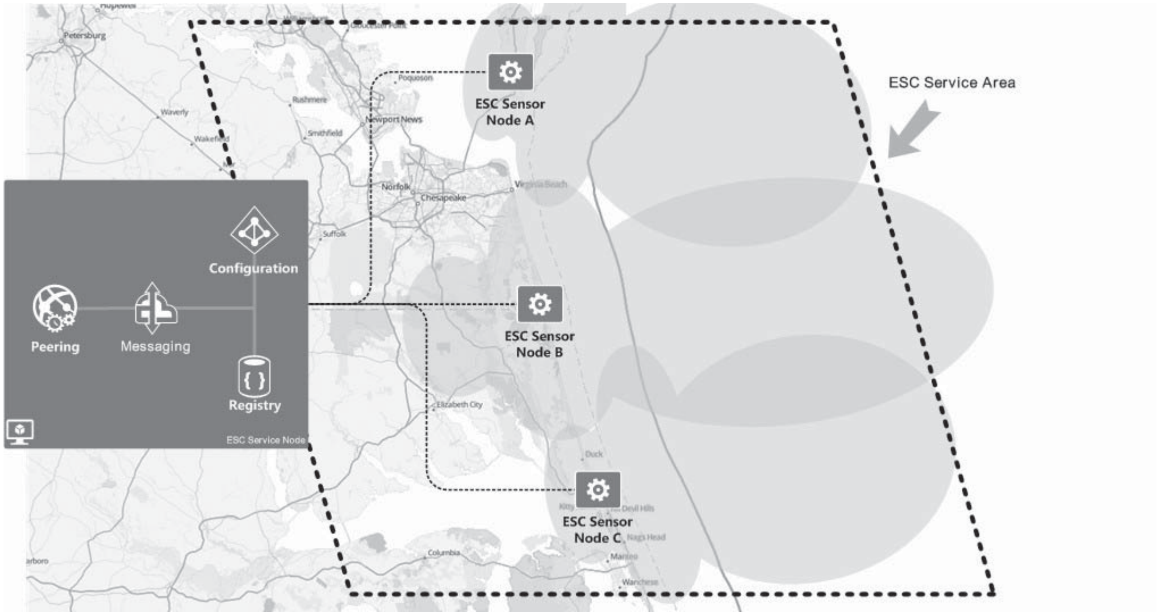


Illustration 13: Service Nodes provide geographically partitioned ESC services.

Referring again to Illustration 13, ESC Sensor Nodes do not communicate or exchange information with other ESC Sensor Nodes in a peer-to-peer arrangement. Instead message routing is organized in a strictly hierarchical configuration where ESC Sensor Nodes receive their start-up and run-time configuration from a *configuration* server, register their available sensing capabilities with a *registry* server, and send spectrum sense information to a *messaging* server. ESC Service Node information to a SAS is then consolidated and routed through a *peering* server, which is the peering gateway to a subscribing SAS and communicates using the SAS Gateway Protocol.

6.3 Geographic Partitioning Strategy

In the Key Bridge ESC Infrastructure the NTIA-defined Exclusion Zones are protected according to a *geographic partitioning strategy*, which is implemented by each ESC Service Node and forms the basis for NIIU detection services presented to a SAS.

The geographic partitioning strategy is established according to a mathematical method wherein a larger, containing geographic region such as the continental United States (CONUS) or the U.S. Mid-Atlantic, for example, is subdivided into many smaller geographic regions. Each of these smaller regions is called a *ESC Service Cell*.

The process of calculating and formalizing ESC Service Cells is expected to occur prior to ESC Service Node and Sensor Node provisioning and commissioning and may be further explained by referring to Illustration 14, where a regular, cellular grid of ESC Service Cells is overlaid upon the ESC Service Area introduced earlier.

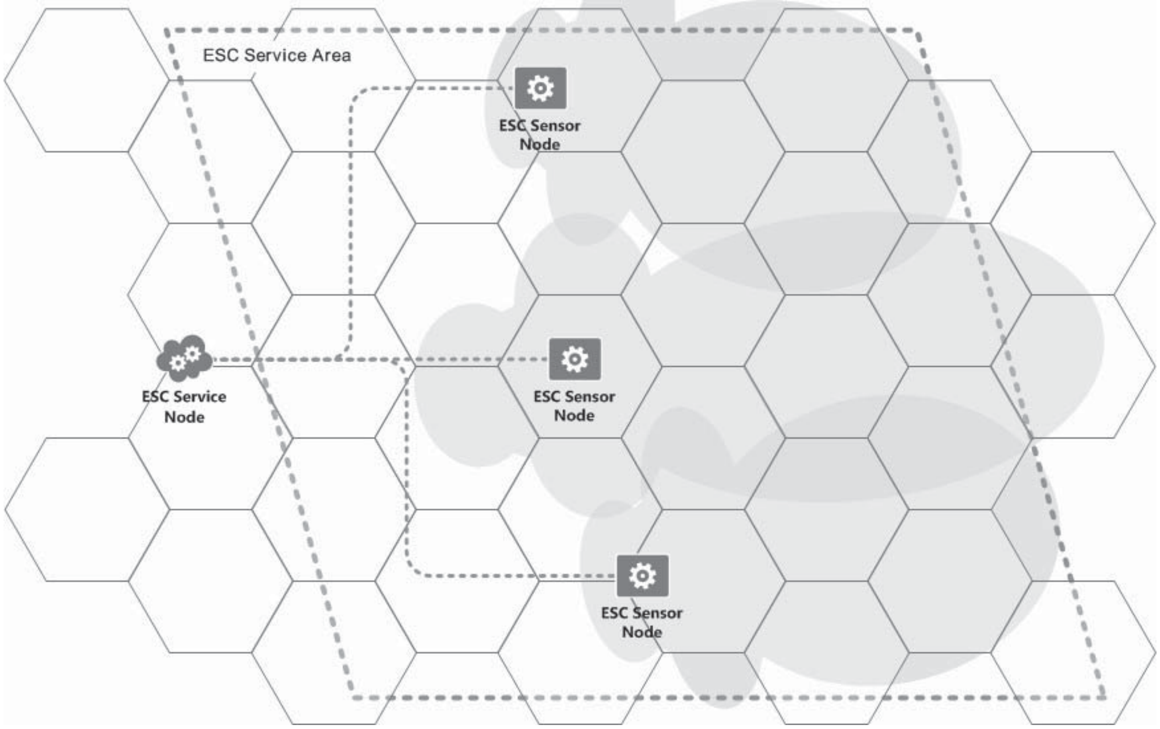


Illustration 14: Geographic partitioning creates ESC Service Cells.

It should be noted that ESC Service Cells may be arbitrarily defined and dynamically adjusted by the ESC administrator and need not be related to or dependent upon a geographic or political boundary; ESC Service Cell configuration and identification may be organized in whatever fashion the ESC finds most convenient. The geographic partitioning strategy to establish a regular grid of ESC Service Cells is also independent of ESC Service Areas, ESC Sensor Node coverage areas, or of NTIA Exclusions Zones, Census Tracts, etc.

A ESC Service Node selectively authorizes or prohibits secondary spectrum use within a each service cell based upon its detection of the presence (or absence) of NIIU spectrum operations. During the normal course of operation a ESC Infrastructure, through its ESC Sensor Nodes, will sense and detect the presence of NIIU spectrum operations. If the ESC determines that the non-informing incumbent is incompatible with secondary or tertiary users operating within a particular service cell the ESC Service Node may then activate (i.e. forbid CBSD operation) or deactivate (i.e. allow CBSD operation) in the service cell.

NIIU location information may be accurately identified by a ESC Sensor Node but no information about the NIIU is shared beyond the ESC Service Node. Rather, NIIU information is internally reduced by the ESC Sensor and Service Nodes into localized ESC Service Cell availability information, which is shared with a SAS. The SAS in turn authorizes or prohibits CBSD operations within the ESC Service Cell identified by the ESC Service Node.

By this method a ESC Infrastructure may cooperate with a SAS to enable CBRS spectrum availability over a large geographic region with adjustable precision while also protecting and not disclosing detailed information about detected NIIU spectrum operations.

When using a geographic partitioning strategy, NIIU protection is effected by a SAS according to the following simple criterion:

> **Rule**: If a ESC Service Area geographically *intercepts* a (NTIA) Exclusion Zone then a ESC Service Node must positively identify a ESC Service Cell as available before a SAS may authorize CBSD operation within that ESC Service Cell's geographic extent.

According to the proposed geographic partitioning strategy a NIIU is detected and protected in the ESC using the following procedure:

- a fixed, cellular grid pattern of ESC Service Cells is established;[14]
- NIIU spectrum operations are detected and evaluated;
- each ESC Service Cell operating permission is updated; and
- the ESC Service Cell remains unavailable until the IU is no longer detected and a hold-down timer has expired.[15]

[14] In this context the ESC service area pattern is envisioned to be a cellular grid dependent based upon upon geographic coordinates and not on empirical values such as, for example, census data or terrain elevation.

[15] Hold-down timer variability is one factor by which the movement or position of a IU may be obscured. See 47 CFR 96.67(c)(7).

6.3.1 Implementation Example

The geographic partitioning strategy concept is shown below in Illustration 15, where a ship borne NIIU is detected by a *ESC Sensor Node*, which through its *ESC Service Node* causes CBSD activity to be disabled in multiple *ESC Service Cells* to protect the NIIU from receiving interference. Note that each service cell is independently enabled or disabled and the ESC Service Node may disable non-contiguous service cells to effect necessary interference protections for the NIIU as the ESC Service Node may determine.

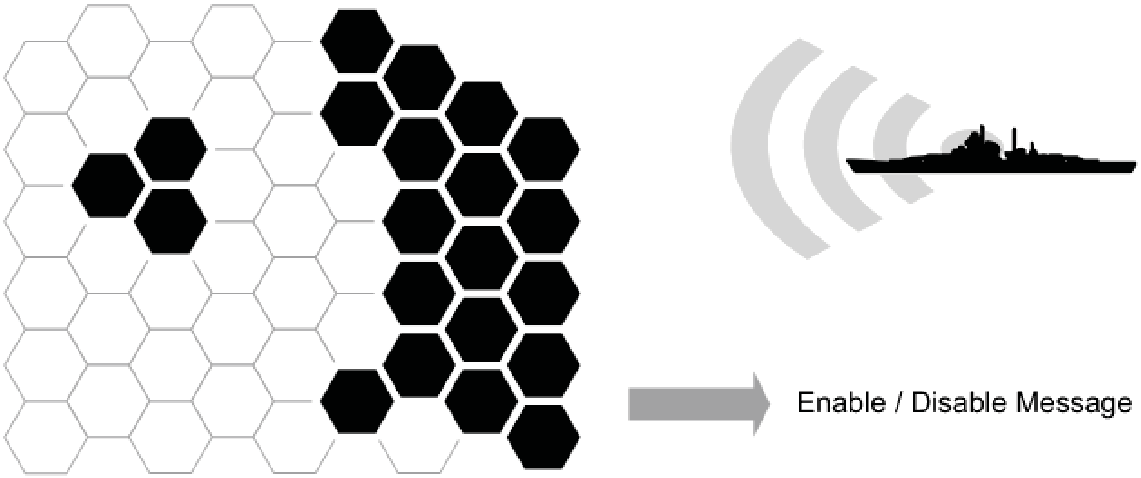


Illustration 15: ESC Service Nodes enable or disable ESC Service Cells.

Continuing the example shown in Illustration 15, the NIIU is detected by a ESC Sensor Node and the NIIU protection requirements are evaluated by the responsible ESC Service Node. The ESC Service Node, by marking service cells as unavailable for service, will cause the responsible SAS to effect CBSD operations in the respective service cells and cause them to cease operation. CBSD operations may be returned after the NIIU is no longer detected, which may also be delayed for a minimum duration defined by a hold-down timer.

Through the use of a geographic partitioning strategy all spectrum information learned from ESC Nodes, including NIIU spectrum profiles, transmitter location, etc., may be contained exclusively within the detecting ESC Nodes.

6.4 Incumbent Sensing and Detection

We describe here two sensing architectures and two mutually compatible detection strategies under development that be believe show promise and that we wish to qualify for NIIU spectrum signal detection and evaluation. The architecture variants are a *fixed sensor network* and a dynamic, *cooperative spectrum sensing* approach, and the strategies are *direct* and *indirect* signal detection.

The architecture and strategy variants and our estimate of the time required to complete development and evaluation of these variants are shown in Table 2.

Architecture / Strategy	**Direct Sensing**	**Indirect Sensing**
Fixed Infrastructure	Phase 1	Phase 2
Cooperative Sensing	Phase 4	Phase 3

Table 2: NIIU sensing and detection architecture and strategies.

Key Bridge proposes to develop, deploy, test and ultimately deploy one or a hybrid combination of these (and possibly other) methods to protect non-informing federal incumbent users in a phased approach, beginning with a conventional direct sensing strategy using fixed infrastructure and subsequently investigating other more sophisticated, cost effective and scalable solutions. We recognize that each strategy is materially different, and expect to forward each solution for evaluation only after it has been proven effective.

We propose a Direct Sensing with Fixed Infrastructure solution. We furthermore propose to subsequently develop and, if feasible, to proffer for evaluation, the following additional combinations of sensing architecture and strategy.

- Indirect Sensing with Fixed Infrastructure
- Indirect Sensing with a Cooperative Sensing Architecture
- Direct Sensing with a Cooperative Sensing Architecture

Key Bridge will develop and to operate two types of ESC Node to effect the direct and indirect architectures: a *ESC Sensor Node*, which includes an embedded sensor apparatus and will be installed and operated as fixed infrastructure, and a *ESC Sensor Fusion Node*, which collects and processes sense data and will be operated in support of a cooperative sensing configuration.

6.4.1 Incumbent Signal Characterization

Radar emission standards for regions outside of the U.S. generally follow the International Telecommunications Union (ITU), which provides methods to compute radar emission masks. Within the United States the National Telecommunications Information Administration (NTIA) governs all US government spectrum use while the US Federal Communications Commission (FCC) oversees non-government spectrum use.

Within the U.S. many different types of radar systems are used in a variety of applications, including avionics, military, automotive, law enforcement, mapping, weather, etc., and all Federal and Military radar systems operate according to guidelines in the NTIA's *Manual of Regulations and Procedures for Federal Radio Frequency Management*, *Radar Spectrum Engineering Criteria* (RSEC).[16]

The radar center frequency may be fixed or variable over time, (i.e. from pulse to pulse), and the radar transmission's instantaneous bandwidth is determined by its pulse modulation, which also determines its ability to resolve targets at different ranges. Radar transmitter peak power can be anywhere from milliwatts to megawatts. These concepts and trade offs are shown in Illustration 16.[17]

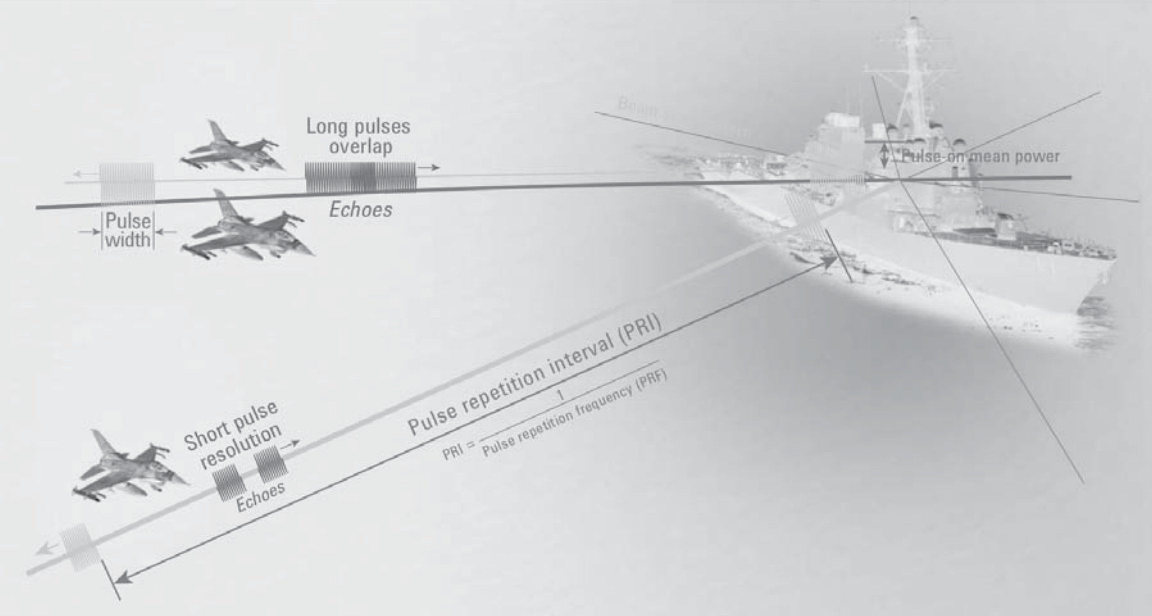


Illustration 16: Radar pulse terminology and trade offs.

Radar system transmissions are generally designed (i.e. modulated) to enable measurement of the

[16] NTIA *Manual of Regulations and Procedures for Federal Radio Frequency Management* (Redbook), Sec. 5.5. See also: Frequency Allocations in 47 CFR Part 2 (FCC Rules and Regulations)

[17] Agilent / Keysight Technologies Technical Note: Radar, EW & ELINT Testing. Fig. 1. Reproduced with Permission.

range relative motion between the radar and a target. Radar signal specifications are determined by application requirements such as range resolution (which is bandwidth dependent), Doppler resolution, maximum ambiguous range, and radar sensitivity. Radar systems typically implement a successive transmission of pulses where the phase or frequency is modulated during the pulse. The radar system is sensing for received signal reflections when not transmitting. Most radar typically have a very small duty cycle (the ratio of time transmitting vs receiving).

6.4.2 RSEC Emission Mask Template

The NTIA RSEC manual specifies, among other things, how to calculate the radar emission bandwidth and suppression levels to generate an applicable emissions mask. The RSEC criteria establish a spectral mask based on a 40 dB bandwidth limit, and the roll-off rates are calculated according to the radar classification. An example is RSEC emissions mask is shown in Illustration 17.[18]

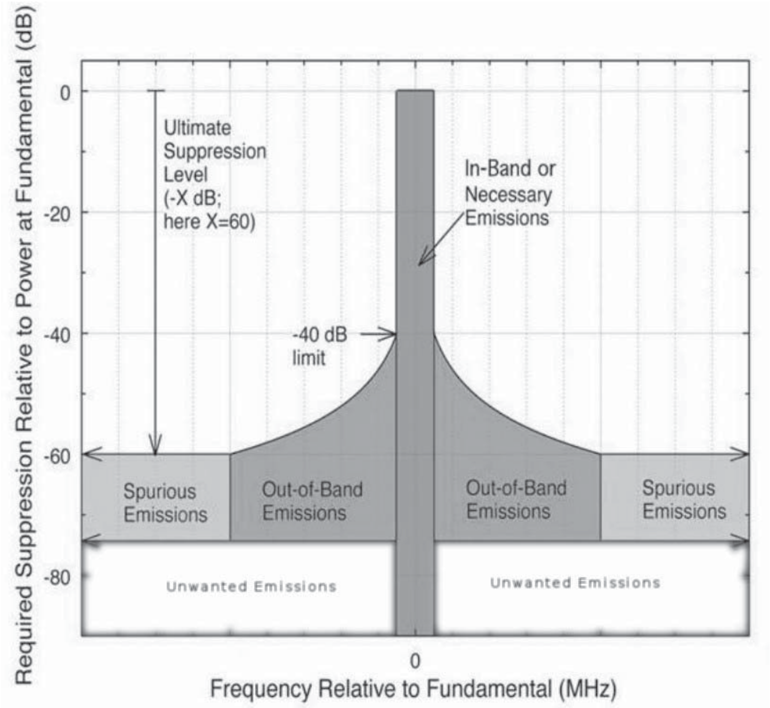

Required Suppression Relative to Power at Fundamental (dB)
0
-20
-40
-60
-80
Ultimate Suppression Level (-X dB; here X=60)
In-Band or Necessary Emissions
-40 dB limit
Spurious Emissions
Out-of-Band Emissions
Out-of-Band Emissions
Spurious Emissions
Unwanted Emissions
Unwanted Emissions
0
Frequency Relative to Fundamental (MHz)

Illustration 17: RSEC emissions mask template.

Radars are divided into five classes in the RSEC: A through E, according to their frequency range, peak power, waveform, and application.

The AN/SPN-43 air surveillance radar is categorized as a IEEE S-band (2-4 GHz) high-power

[18] RSEC emission mask template from Richards, Scheer, Holm, *Principles of Modern Radar: Basic Principles*, Ch. 10.

Group C radar and is governed by RSEC Criteria C.[19] Technical information about the AN/SPN-43 Air surveillance radar is included in an Appendix, and a empirical spectrum sample is shown below in Illustration 18.'[20]

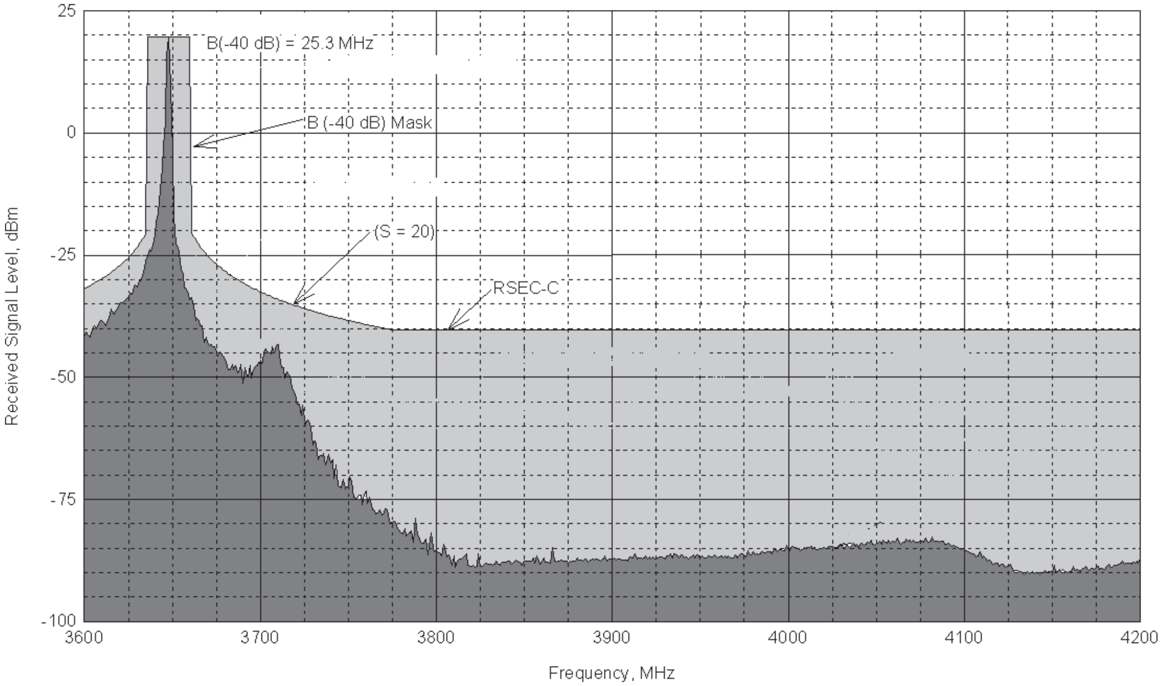


Illustration 18: RSEC Criteria C non-FM pulse radar emission profile.

In general all expected radar emission in the 3.5 GHz band should not exceed the limits established by the RSEC mask, and Key Bridge expects to use the RSEC as a general RF engineering guideline for our deployed sensor apparatus.

[19] The AN/SPN-43's high output power marks it as a Group C radar, described as "All radars not included in Group A, B, D, or E".

[20] From Robert Hinkle, NTIA Office of Spectrum Management, "A Review of the Radar Spectrum Engineering Criteria", with analysis of radionavigation radar emissions in the 3.5 GHz band.

6.5 Direct Sensing Methodology

Key Bridge proposes to develop a *ESC Sensor Node* that will implement mathematically robust direct spectrum sensing methodology based upon existing best practice to detect federal transmissions and to determine that the spectrum needs to be evacuated.

Various methods to detect, measure and classify (i.e. positively identify) a pulsed radar emission are known. Various mathematically robust methods are known and commercial products are available to implement pulsed radar emission detection that will satisfy the requirements of Part 96 ESC operation. Key Bridge does not believe significant technology development work is required to accomplish this task. Some examples of relevant theoretical work in this field are identified in Section 9 (Bibliographic References).

If necessary, Key Bridge can implement a transmitter location methodology based upon existing best practice. Various mathematically robust methods are known and commercial products are available to implement pulsed radar emission location. Key Bridge does not believe significant technology development work is required to accomplish this task. Some examples of relevant theoretical work in this field are identified in Section 9 (Bibliographic References).

In addition to a robust theoretical foundation, a mature commercial test and measurement hardware and software ecosystem exists for radar system development, design and detection. Key Bridge believes that implementing and operating a distributed radar sensing and detection capability does not require significant original engineering or design work, but rather may be accomplished through the integration and scaled deployment of commercial off-the-shelf technologies and systems.

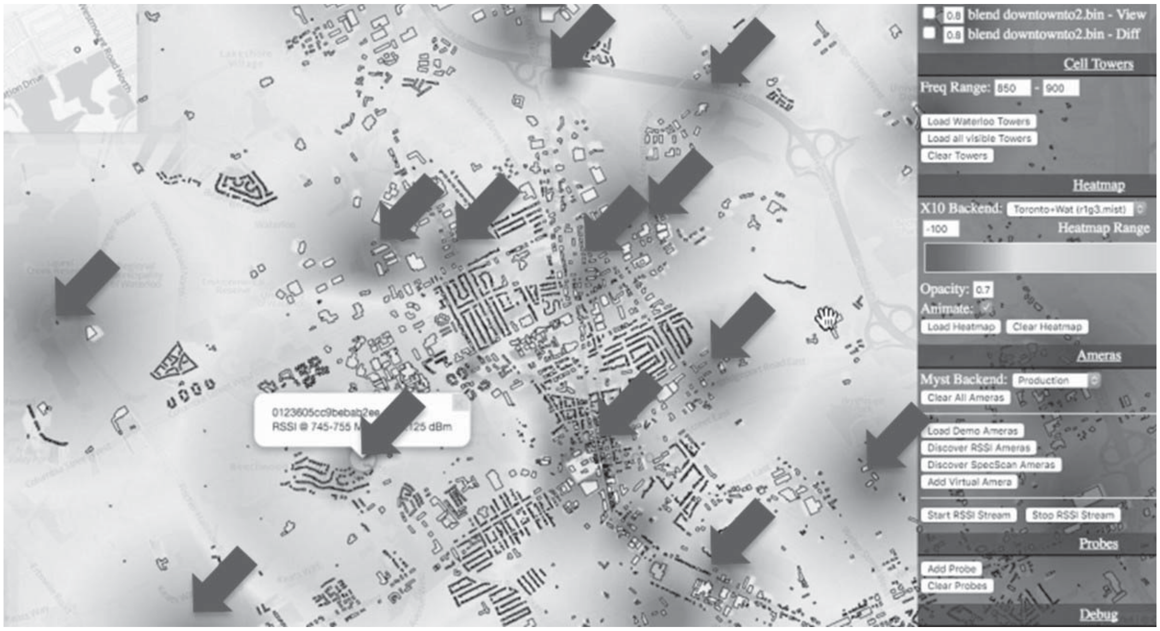
6.6 Indirect Sensing Methodology

In addition to the conventional direct incumbent sensing and detection strategies described in section 6.5 (Direct Sensing Methodology), Key Bridge also proposes to develop and pursue an alternative *indirect* approach to protecting non-informing incumbent user spectrum operations through the concept of *negative correlation*.

Negative correlation works according the following basic principal:

- If all non-incumbent transmitters are known, than any unknown transmitter should be an incumbent.

In a negative correlation configuration a ESC attempts to *affirm* that all detected signals are known, and causes a SAS to effect interference protection for any *negatively* correlated signal; that is, a signal that it does not recognize or may not directly detect, but whose existence is indicated through negative correlation with known metrics. This concept is be colloquially termed "protect all strangers" and begins by first identifying and locating all known transmitters,then proceeds to classify and protect valid unknown or unrecognized transmitters. This concept is shown in Illustration 19, where numerous known transmitters and a single unknown transmitter have been identified and located in collaboration with a SAS transmitter database.[21]


0123605cc9bebab2ee
RSSI @ 745-755 M 125 dBm

☐ 0.8 blend downtownto2.bin - View
☐ 0.8 blend downtownto2.bin - Diff

Freq Range: 850 - 900
X10 Backend: Toronto+Wat (r1g3.mist)
-100 Heatmap Range
Opacity: 0.7
Animate: ✓
Myst Backend: Production

Illustration 19: Identification of known transmitters enables indirect sensing.

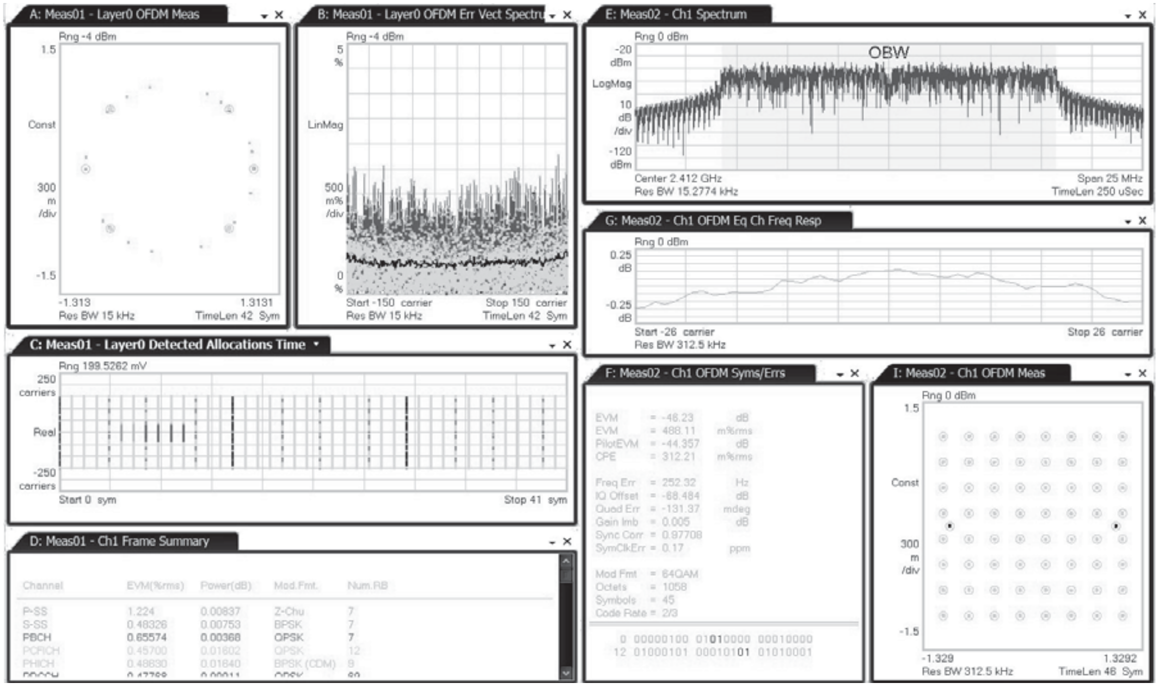
Key Bridge proposes to employ *vector signal analysis* (VSA) to aid in the rapid identification and classification of digital signals and to correlate those detected signals to known CBRS

[21] Reproduced with Permission, Courtesy of Cognitive Systems Corp.

transmitters.[22] In this task we expect to follow the ITU Recommendation ITU-R SM.1600 “Technical Identification of Digital Signals” for collection of IQ data and signal analysis. ITU-R SM.1600 describes the following general process of digital signal identification:

- evaluation of external signal characteristics;
- when low or partial a priori knowledge is available about the signal, conduct an inspection of internal signal characteristics such as modulation type and other waveform parameters;
- when strong a priori knowledge is available about the signal, correlate with known waveform characteristics;
- compare the measured signal demodulation, decoding and comparison with known waveform characteristics,.

An example screen shot of a VSA software application presently under evaluation for this task is shown in Illustration 24.[23]



```
EVM       =  -46.23    dB
EVM       =  488.11    m%rms
PilotEVM  =  -44.357   dB
CPE       =  312.21    m%rms

Freq Err  =  252.32    Hz
IQ Offset =  -88.484   dB
Quad Err  =  -131.37   mdeg
Gain Imb  =  0.005     dB
Sync Corr =  0.97708
SymClkErr =  0.17      ppm

Mod Fmt   =  64QAM
Octets    =  1058
Symbols   =  45
Code Rate =  2/3

 0  00000100  01010000  00010000
12  01000101  00010101  01010001
```

Channel	EVM(%rms)	Power(dB)	Mod.Fmt.	Num.RB
P-SS	1.224	0.00837	Z-Chu	7
S-SS	0.48326	0.00753	BPSK	7
PBCH	0.65574	0.00368	QPSK	7
PCFICH	0.45700	0.01602	QPSK	12
PHICH	0.48630	0.01640	BPSK (CDM)	9
PDCCH	0.47768	0.00011	QPSK	80

Illustration 20: Vector signal analysis software for digital signal identification.

The ESC Sensor Nodes that Key Bridge intends to develop and deploy will have the ability to readily detect all types of digitally modulated signals in the 3.5 GHz band, and the VSA software

[22] §96.41(a) requires and Key Bridge therefore expects that all known CBRS transmitters will employ digital modulation. The described method is greatly simplified by, but does not absolutely require, the use of digital transmission.

[23] Reproduced with Permission, Courtesy of Keysight Technologies, Inc.

will be able to positively identify any detected digital signal. Furthermore, Key Bridge ESC Infrastructure, in cooperation with a SAS, *should* be able to correlate detected digital signals with individual CBRS transmitters. With this information and in such a cooperating configuration Key Bridge ESC Infrastructure *should* be able to affirm that all detected signals are known, and that a unknown and unrecognized (non-digital) signal is very likely a non-informing incumbent.

Note that in the above description we twice employ the subjunctive term “should.” Key Bridge believes our “protect all strangers” approach to ESC operation shows great promise in theory, and we hope to develop and prove (or disprove) its feasibility after receiving designation as a ESC administrator.

An obvious inherent weakness in a indirect, negative correlation strategy is its potential susceptibility to abuse from a malicious, unauthorized transmitter. Key Bridge believes that this risk may be mitigated by establishing bounding conditions on the expected nature of “strangers” that should be considered to indicated incumbent activity. This is an topic of research we wish to further develop.

6.7 Fixed Infrastructure Sensing Apparatus

The Key Bridge team is still developing the sensing hardware component of our *ESC Sensor Node*. Sensing hardware components used within a ESC Sensor Node will be configured to accept, at minimum, the maximum expected received power calculated using available AN/SPN-43 technical parameters and a corresponding RSEC-derived emission mask.

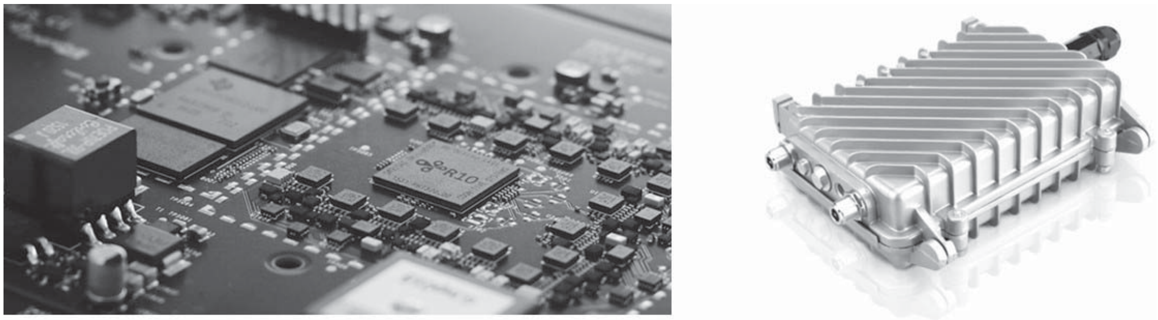


Illustration 21: Example ESC Sensor Node with detection and processing capabilities.

A Key Bridge / Cognitive Systems ESC Sensor Node implementation is shown in Illustration 21.[24] The Key Bridge ESC Sensor Node is based upon the Cognitive Systems R10 integrated software defined wireless processor and G10 reconfigurable front-end. A typical Cognitive Systems R10 hardware chip configuration is shown in Illustration 22.[25]

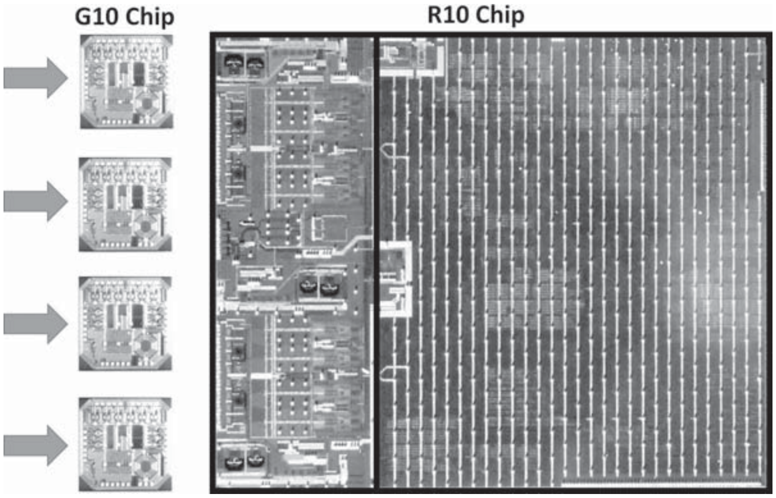


Illustration 22: The Sensor Node is a software defined radio on a chip.

The R10 processor includes embedded, hardware-bases cryptographic keys, a dual-MIMO

[24] Reproduced with Permission, Courtesy of Cognitive Systems Corp.

[25] Id.

software defined radio and dual vector processors to implement digital signal processing and analysis.

In the ESC Sensor Node configuration the R10 processor is configured to load and execute wireless signal processing, classification and identification algorithms. Upon designation as a ESC administrator Key Bridge can supplement this proposal with additional hardware performance details including:

- on-board data processing capabilities;
- hardware tamper resistance;
- sensing thresholds;
- sensor sensitivity;
- resiliency to receiver front-end saturation and burn-out; etc.

6.8 Cooperative Sensing Methodology

In addition to a ESC Sensor Node, which includes an embedded sensing apparatus, Key Bridge proposes to develop a *ESC Sensor Fusion Node*, which receives and processes signal information from external sensor devices to determine the presence or absence of a non-informing incumbent user through a *cooperative sensing methodology*.

In the 3.5 GHz band CBSD secondary (or tertiary) users may exploit spectrum resources when a primary user (PU) is absent, but must rapidly vacate the spectrum when the primary user returns to operation. Effective spectrum sensing is therefore a critical task for CBSD cognitive radio networks. Cooperative spectrum sensing can be an effective method to identify certain types of incumbent signals and also to resolve the presence of digitally modulated secondary (or tertiary) hidden nodes.

Energy detection methods are optimal for detecting zero-mean constellation signals if prior knowledge of the digitally modulated signal is not known. Non-modulated incumbent signals such as a pulsed radar, for example, may be detected in a time-division duplexed (TDD) system by coordinating a periodic listening window, or "quiet time".[26]

Energy detection can provide accurate sensing performance when the signal-to-noise ratio (SNR) is high, and cooperative spectrum sensing may be employed to improve overall spectrum sensing performance and hidden node detection, which are characterized by very low SNR.[27]

Cooperative spectrum sensing and its use in cognitive radio systems and networks is a relatively new area of research. There exists a emerging body of published research on this topic that include a diverse variety of methods and strategies to detect and measure known and unknown transmissions. Some of the more interesting and promising examples of relevant theoretical work in this field are identified in Section 9 (Bibliographic References).

Key Bridge proposes to develop, implement and to evaluate the efficacy of cooperative spectrum sensing methodologies to detect federal transmissions in a ESC Infrastructure. As part of this work, Key Bridge will also consider and evaluate the information and operational security aspects of a distributed, cooperative spectrum sensing approach.

If the results of this work bear fruit Key Bridge will proffer for FCC (plus NTIA and DoD) certification a cooperative spectrum sensing methodology implemented as a *ESC Sensor Fusion Node*.

[26] This is the principal underlying dynamic frequency selection (DFS) techniques in the 5250 to 5350 MHz and 5470 to 5725 MHz bands , a single-sensor technique we hope to improve upon through the use of ESC coordinating control channels.

[27] D. Cabric, S. M. Mishra, and R. W. Brodersen, "*Implementation issues in spectrum sensing for cognitive radios*" in Proceedings of Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, Nov. 7-10, 2004, pp. 772 - 776.

6.8.1 Cooperative Sensing Theory of Operation

Cooperative spectrum sensing seeks to exploit the spatial correlations within sense data collected over a distributed geographic area. The data processing architecture can be centralized for global visibility or partitioned to accommodate limited computing resources or information security requirements.

CBSDs with spectrum sensing capability may be configured to perform cooperative spectrum sensing and organized into a *cognitive radio wireless sensor network* (CR-WSN), which is a specialized ad-hoc network of distributed wireless sensors equipped with cognitive radio capabilities. Research on CR-WSNs is still in its infancy but progressing rapidly.

A CR-WSN is substantively different from conventional wireless sensor networks and also from conventional distributed cognitive radio networks. Research shows that a CR-WSN can achieve performance results greater than the sum of its parts but also requires a high-degree of cooperation to achieve its desired task. Nodes in the CR-WSN must quickly and securely exchange sensing data, which must be correctly and efficiently routed, interpreted, fused and exploited to protect incumbent users.

In a Key Bridge ESC cooperative sensing configuration a secure control channel is established between a ESC Fusion Node and various participating CBSDs. CBSD participation may be organized and coordinated with a SAS or via some other administrative mechanism. CBSD to ESC communications in a cooperative sensing configuration are event driven and message based.

- A ESC Sensor Fusion Node organizes spectrum sensing by signaling, either directly to individual CBSDs or indirectly via a SAS, the desired sensing configuration, which includes the frequency range that a CBSD should tune to, the desired sensing duty cycle, and a synchronized timing information.
- CBSDs report collected sensing information to the ESC Sensor Fusion Node.

The quantity and quality of reported data may vary by device, and data analysis and interpretation techniques are the subject of continuing research. CBSD messages to a ESC Sensor Fusion Node may be regular and periodic or occasional and only sent when triggered by a state change condition. For example, a CBRS may send a received signal strength indicator (RSSI) to the ESC Node every 10 seconds. In another example a CBRS may notify the ESC Node only when a non-modulated, pulsed signal is detected. Alternatively, a CBRS may notify the ESC Node when its signal quality degrades beyond a certain level, which may indicate the presence of a high-power interfering signal such as an incumbent radar.

In a envisioned Key Bridge CR-WSN individual CBSDs collect environmental spectrum *data* and forward the data to a ESC Sensor Fusion Node for processing. Only within the ESC Sensor Fusion Node is the data transformed into *information* and analyzed to determine the presence or absence of an incumbent user. Once a ESC Sensor Fusion Node has determined the presence or absence of a (non-informing) incumbent user the ESC Node causes the incumbent user to be protected by conventional methods; namely by updating the availability status of certain ESC Service Cells and informing the SAS of the changed availability status of those Areas.

A ESC Sensor Fusion Node receives spectrum sense data and/or spectrum sense event messages from each enrolled / participating CBSD. An example configuration showing three clusters of CBSDs in a cooperative spectrum sensing configuration is shown in Illustration 23.

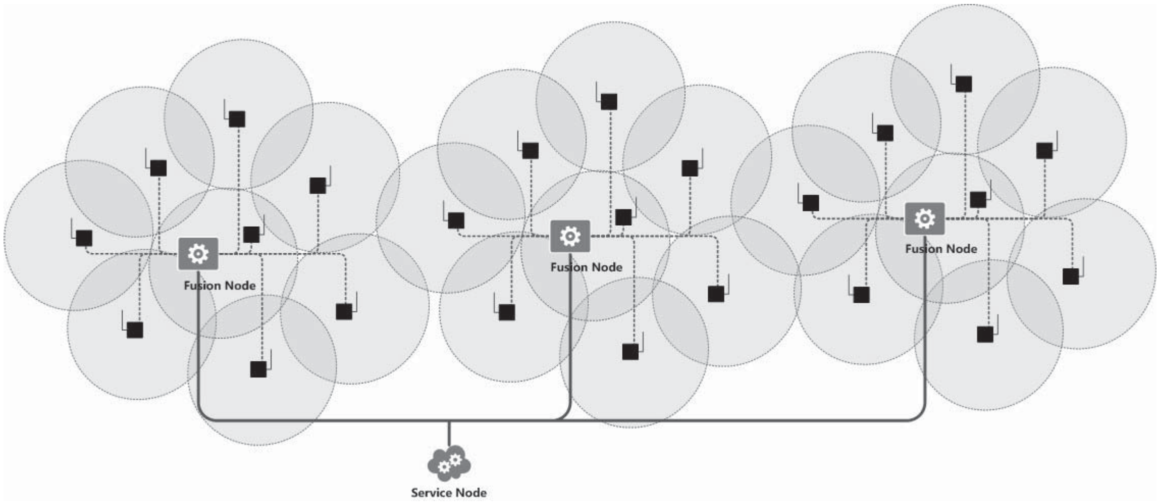


Illustration 23: ESC Sensor Fusion Nodes organize Cooperative Spectrum Sensing.

In this arrangement the CBSD does not act upon the sensed data, but rather only forwards the sense data for processing by the ESC Sensor Fusion Node. The SAS retains full responsibility for instructing a CBSD configuration change.

A cooperative wireless sensor network may consist of hundreds or thousands of CBSDs and their corresponding end user devices deployed throughout an extended geographic region. The SAS responsible for that geographic region may collect and route messages between a ESC Sensor Fusion Node and individual CBSDs or may invite direct CBSD to Fusion Node messaging.

Spectrum sensing is a key element in all cognitive radio networks as it is generally performed before allowing unlicensed (i.e. secondary) users to access the vacant licensed channel. SAS + ESC facilitated control channel messaging presents a method by which heterogeneous cognitive radio systems may implement cooperative spectrum sensing to effectively identify hidden nodes.

When also coordinated through a ESC, SAS facilitated control channel messaging may be used to coordinate periodic listening windows across a geographic region to implement a distributed pulsed radar detection algorithm.

6.9 Modeling and Computing Spectrum Coexistence

IEEE 1900.5.2, the *Draft Standard for Method for Modeling Spectrum Consumption*, describes a generalized method for modeling the consumption of any type of use of RF spectrum. The standard defines an analytical framework and data modeling strategy that may be used to express the boundaries of spectrum consumption by any transmitting or receiving device.

Since 2014 Key Bridge has made significant contributions to the IEEE 1900.5.2 working group, with particular interest to use this standard in a 3.5 GHz SAS and ESC.

Spectrum consumption models naturally lend themselves to efficient evaluation and calculation of spectrum coexistence and identification of risks for potential interference between spectrum users. Any conceivable type and configuration of spectrum consumer may be modeled, including transmitters, receivers, fixed stations, mobile stations, terrestrial networks, aerial platforms, continuous carriers, pulsed signals, frequency hopping waveforms, etc.

The current draft standard includes mathematically robust and repeatable computational methods for arbitrating coexistence between and amongst different *transmitter* and *receiver* models. Using IEEE 1900.5.2, incumbent radar systems may be readily modeled and coexistence calculations and analysis executed against individual CBSDs, CBSD wireless networks, and the aggregate transmission effect from geographically selected populations of CBSDs.

6.9.1 Modeling Transmitters

A IEEE 1900.5.2 *transmitter model* describes the extent and strength of the transmitter radio frequency emission over a geographic region. This model defines the transmitter's emission and geographic service or signal coverage area from the transmitter's perspective. An example path loss plot is shown in Illustration 24, which shows a simplified decrease of signal power versus (radial) distance from the transmitter. The actual modeled path loss is highly configurable, and detailed later in 6.9.3 (Modeling Signal Propagation).

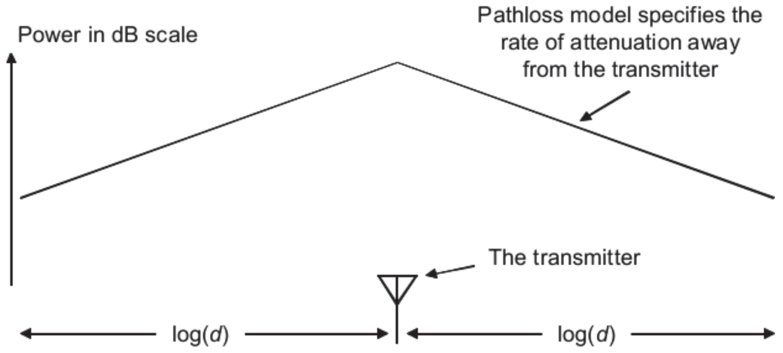

Power in dB scale
Pathloss model specifies the rate of attenuation away from the transmitter
The transmitter
log(d)
log(d)

Illustration 24: A modeled transmitter emission.

A transmitter model includes information about the transmitting device's spectral, spatial and temporal range of use, plus geolocation information to identify where a fixed transmitter may be operated or within which region a mobile transmitter may be expected to operate. Signal levels across a geographic region are projected using a simplified path loss model.

6.9.2 Modeling Receivers

A IEEE 1900.5.2 *receiver model* describes the receiver's sensitivity over a geographic region. This model, from the receiver's perspective, defines compatible transmitter configurations or, alternatively, incompatible interference conditions to the receiver. An example sensitivity plot is shown in Illustration 25, which shown increasing sensitivity for locations closer to the receiver.

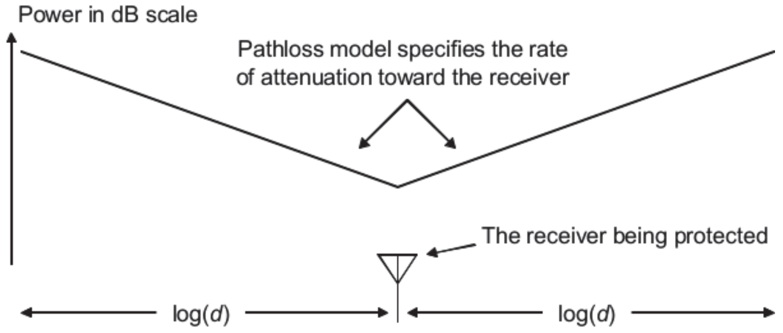

Power in dB scale
Pathloss model specifies the rate of attenuation toward the receiver
The receiver being protected
log(d)
log(d)

Illustration 25: A modeled receiver sensitivity.

A receiver model identifies a minimum required receive signal power and the location where a fixed receiver may be located or a geographic region where a mobile receiver may be expected to operation, plus a simplified propagation model that other parties may use to establish suitable protection for the describe receiver.

6.9.3 Modeling Signal Propagation

Emissions attenuate as they propagate away from their source, and the quantity of attenuation is a function of frequency, distance, and the environment. Precise prediction of attenuation is usually a difficult, computationally intensive task and can vary significantly by minor configuration changes and subtle environmental effects. Commonly use models include ITU-R P.1546, Longley Rice and Okumura-Hata.

The utility of the conventional radio path loss and signal propagation models depend heavily upon an accurate digital elevation model, and large libraries of static data are not amenable to use in real-time systems or in distributed applications. There is therefore great incentive and utility in avoiding ESC dependencies on external terrain model data. The IEEE 1900.5.2 standard handles this complexity and eliminates third-party terrain model dependencies by trading a slight loss of precision with significant simplification and increase in mathematically robustness and repeatability. This is accomplished by modeling signal propagation with a user-configurable piecewise linear log-distance path loss model.

Several example configurations are shown in Illustration 26, where the piecewise linear model parameters are adjusted (by the modeling user) to best match their calculated optimal result for four different configurations. This best-fit matching process can be automated.

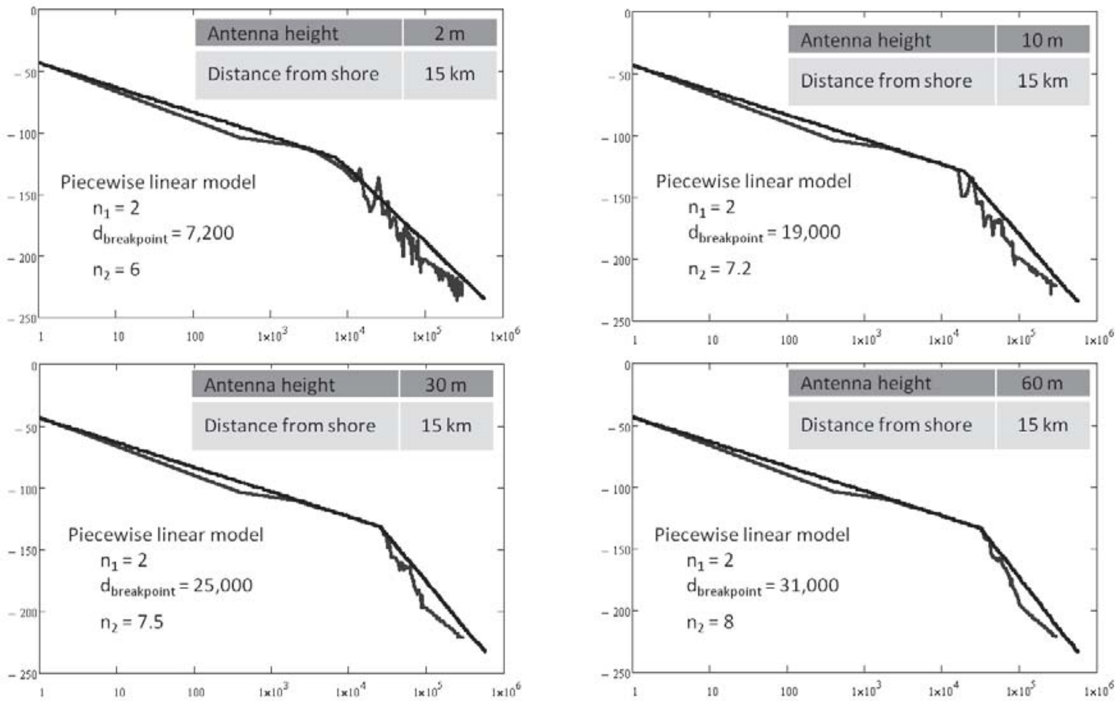


Illustration 26: Modeled signal propagation to match different configurations.

A transmitter path loss model, and its inverse: a receiver sensitivity model, describe their desired attenuation of RF emissions versus distance. This attenuation may be extended across a geographic area or region.

The transmitter or receiver model creator (i.e. the transmitter or receiver device owner) may adjust their (simplified) propagation model to suite, possibly by comparing the modeled propagation with their chosen optimal solution, to achieve the closest acceptable fit for their specific situation. The optimal solution may be any conventional terrain-data dependent path loss model, such as ITU-R P.1546, Longley Rice, Okumura-Hata, etc.

6.9.4 Computing Spectrum Coexistence

IEEE 1900.5.2 spectrum consumption models are readily extended to networks, systems and geographic exclusion or protection zones to evaluate coexistence and calculate compatible configurations and spectrum use policies for any combination of transmitter and receiver.

The interaction of transmitter and receiver models may be used to determine, generally, whether the devices are compatible (i.e. may communicate with each other) or the propensity of the two modeled systems to interfere with each other. For example, if the predicted power from a modeled transmitter at the location of a modeled receiver is below the interference threshold established by the receiver then the transmitter – receiver pair may be deemed compatible (i.e. the devices may coexist).

A single transmitter and a single receiver configuration produces a 1900.5.2 computation similar to a classic link budget calculation. The modeled transmitter and receiver combination also provides a power margin that indicates whether and to what extent the receiver will experience interference from the transmitter. Further calculations may determine a maximum allowable transmit power below which the transmitter – receiver pair can reasonably coexist. This is detailed in the IEEE specification and a general representation is shown in Illustration 27.

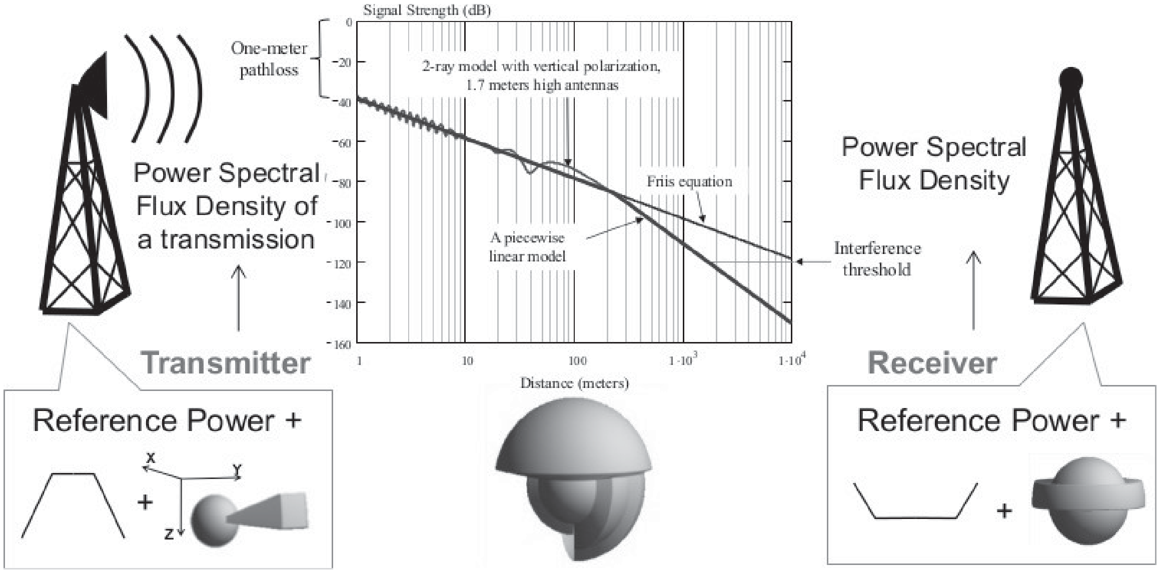


Illustration 27: Assessing compatibility using spectrum consumption models.

The proposed coexistence methodology may be readily extended to collections and networks of transmitters and receivers of arbitrary configuration to approximate and calculate the effect and risk of *aggregate interference*.

IEEE 1900.5.2 spectrum models may be furthermore employed to facilitate coexistence and spectrum sharing by conveying to the modeled transmitters and receivers any changes to their respective configuration that if implemented would effect compatibility. In the instance of incumbent to non-incumbent coexistence this the conveyed change is for the non-incumbent transmitter to cease operation.

Key Bridge proposes to employ 1900.5.2 spectrum models to calculate the coexistence status of non-incumbent CBSD transmitters. While the exact implementation details are presently under development, the methodology generally conforms to the following procedure:

1. The incumbent radar transmitter is modeled according to the maximum possible transmission configuration as specified in the NTIA RSEC manual.

2. All CBSD receivers in a ESC Service Cell are consolidated into a single model having no tolerance for radar signal acceptance, the tolerance increasing with distance from the service cell location. This is called a *CBSD Radar Acceptance*.
3. The measured incumbent signal power is estimated and the incumbent transmitter distance from the ESC Service cell is estimated.
4. If the measured power is above the CBSD Radar Acceptance plot then CBSD operations are disallowed within the cell

It should be noted that the exact configuration of the *CBSD Radar Acceptance* is determined by the aggregate interference effects of the ESC Service Cell's CBSD *transmitter* population on a modeled incumbent radar *receiver*. This is the subject of continuing work and not yet specified.

The proposed methodology may be visually explained by reference to Illustration 28, where a ESC Service Cell CBSD Radar Acceptance curve is plotted showing acceptable power vs. distance.

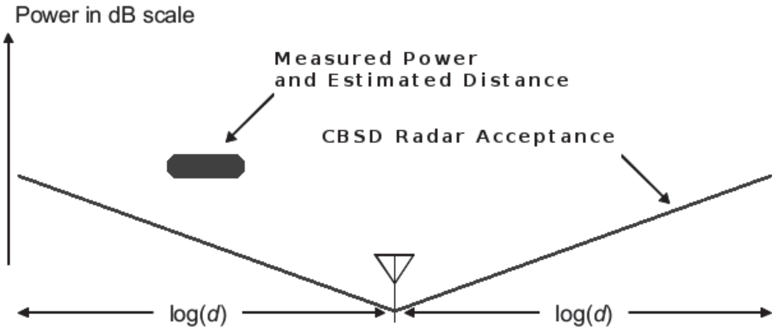


Illustration 28: CBSDs have no incumbent signal acceptance.

A incumbent radar signal measured power and estimated distance may also be rendered on the same power vs. distance chart. Coexistence between the measured signal and the modeled ESC Service Cell can be readily established by determining whether the radar's *Measured Power and Estimated Distance* point is above or below the *CBSD Radar Acceptance* curve.

Referring again to Illustration 28 the measured radar point is actually an extended area to indicate some degree of uncertainty. Nevertheless the *Measured Power and Estimated Distance* area is clearly above the *CBSD Radar Acceptance* curve and indicates that CBSD operations in the ESC Service Cell must be disallowed.

By employing IEEE 1900.5.2 modeled path loss a ESC Sensor Node, and by extension the ESC Infrastructure, can implement mathematically robust, repeatable and predictable protections for non-informing incumbent users.

7 Key Bridge ESC Security Architecture

Envisioned ESC operations are, by definition, a form of signals intelligence. This is complicated by the fact that in the 3.5 GHz band the NIIU is the U.S. Military. Accordingly, a ESC implementation may be expected to operate under heightened information and operational security constraints.

The Key Bridge ESC Infrastructure solution enforces a *positive security model* to prevent unauthorized access, protect sensitive data and limit the effects of a potential breach, attach or failure. In computer security a positive security model is also called as "white list" and defines *a priori* all allowed conditions while rejecting everything else. This contrasts with a negative (i.e. “black list”) security model which attempts to identify and filter what is explicitly disallowed while implicitly allowing everything else.

The Key Bridge ESC Infrastructure positive security model is implemented using *security domains*.

7.1 Security Domains

In information security a *security domain* is an enclave of computer applications that are kept separate from other applications. Within a security domain applications are typically configured to trust one another and may freely communicate. In a networked environment different security domains may be created using firewalls to limit communication with other domains. In a cloud-based operating environment security domains can be dynamically established using virtual networks and virtualized firewall configurations.

The Key Bridge ESC Infrastructure security domains are created based upon *functional isolation* and *logical segmentation.*

- **Functional isolation** is a system security technique that groups applications and computer systems with similar functionality and security threats profiles into a dedicated security enclave. It allows the application of tailored security profiles to counter known threats and limit the possible impact of unknown threats.
- **Logical segmentation** supervises resource availability for applications. Logical segmentation creates security communities across system components without regard to their physical location. It creates a flexible, layered security approach based on applications, application groups, IP addresses and geographic regions and allows the creation and application of tailored security profiles to isolated applications and computer systems.

Logical segmentation has several key benefits, principal among them the ability to pinpoint and prevent attacks at a very fine level. It provides a robust method to prevent "pivot" attacks, where one compromised service is exploited to attack others. This concept is shown in Illustration 29, where multiple ESC Service + Sensor Node configurations are logically partitioned into enclaves.

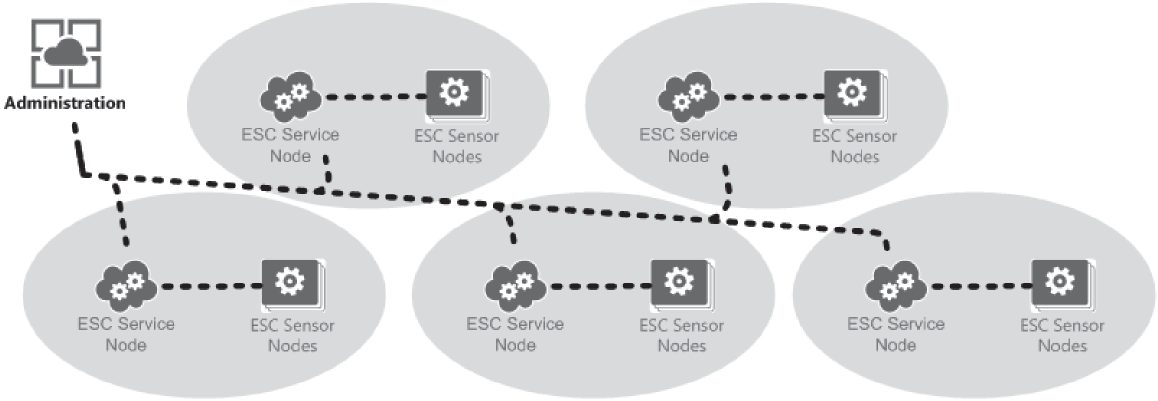


Illustration 29: ESC Infrastructure is logically segmented into security enclaves.

The Key Bridge ESC security solution has tremendous flexibility in this respect; it accommodates data security at the physical and logical networking layers, in between security enclaves, and between the various service applications.

The inherently distributed nature of ESC Infrastructure provides a natural guide to implement a geographically-based logical partitioning strategy. In the Key Bridge ESC Infrastructure applications are logically segmented by geographic region. More specifically: by ESC Service Area, where each ESC Service Area is a security enclave and contains one ESC Service Node plus the ESC Sensor Nodes under local management and control.

Overlaid onto this logical partitioning of enclaves is a functional partitioning of security domains. The Key Bridge ESC Infrastructure is modeled with three functional security domains, each allowing a different scope of communication for their respective applications. These domains are: *data*, *service* and *administration* and their relationship is shown in a Venn diagram in Illustration 30.

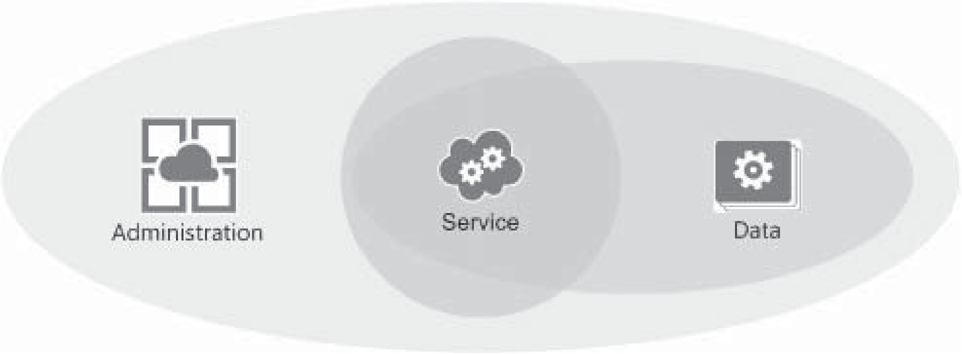


Illustration 30: ESC security domains logically intersect.

- **Data**: A data security domain is created to protect communications between a ESC Service Node the various ESC Sensor Nodes that it manages and controls. RF sensing data and raw spectrum information exchange is limited to the data security domain.
- **Service**: A service security domain is created to protect communications between the various applications that make up a ESC Service Node. Detailed operating configurations and policies are configured at the service node level.
- **Administration**: An administration security domain provides for global monitoring of system health and performance plus configuration of high-level operating configurations and policies.

Each connection between enclaves in the security architecture represents a policy enforcement point where Key Bridge may enforce granular control of application and message traffic, pinpoint anomalies, and prevent undesired activity either from internal mis-configuration or malicious act. One such policy is the type of communication allowed between the Administration and Data enclaves.

The *administration security domain* allows direct and message-based communications between applications in the Administration and Service security domains and only limited communication with the Data security domain. This is concept is shown in Illustration 31.

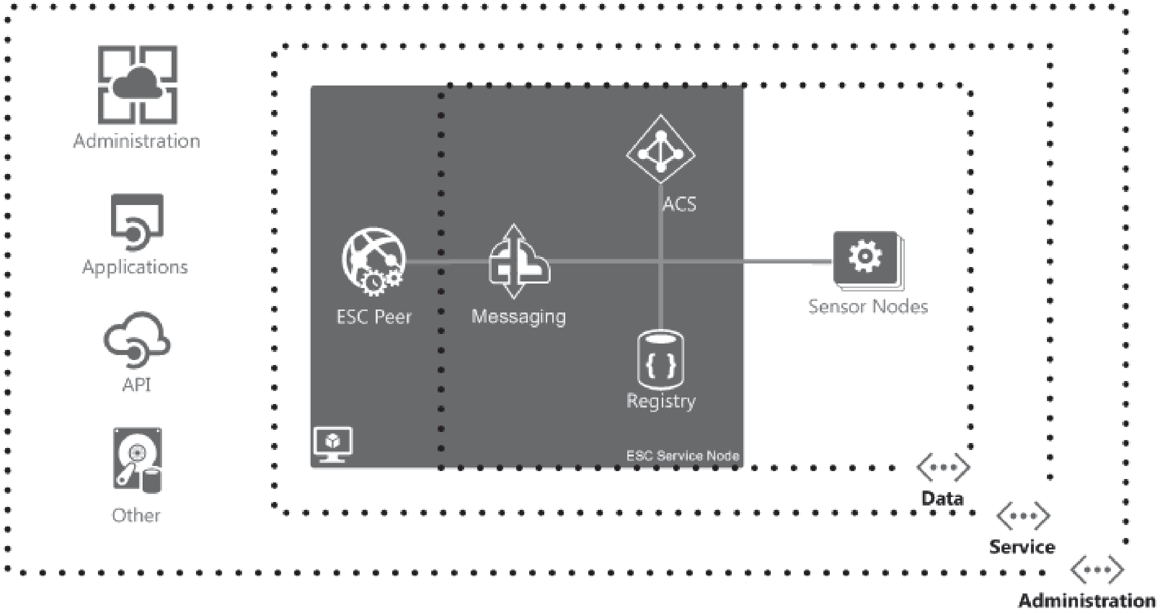


Illustration 31: ESC Infrastructure incorporates layered security domains.

A application in the Administration domain, such as the ESC Administration Portal, may communicate with, interrogate and receive operating information from devices and applications in the Service and Data security domains, but may not receive spectrum data because spectrum sensor data is limited to the Data security domain of its originating ESC Sensor Node. In this regard the administration security domain may be considered as an *in-band control plane* enabling message exchange for system management, centralized logging and auditing plus API and other applications requiring global scope.

7.2 Communications Security

Messages received from the Internet cannot be trusted by default, and the Key Bridge ESC Infrastructure positive security model does not allow connections or communications with unknown parties. The Key Bridge ESC employs several procedures and technologies to ensure system security. These include:

- Only authorized Sensor Nodes may connect to Service Nodes
- All Nodes employ mutual authentication
- Insecure communications are not allowed
- All communications between enclaves is protected by Transport Layer Security (TLS) or IPSEC
- Messages must have end-to-end protection and use *WS-Security* for authentication, integrity and confidentiality procedures

The Key Bridge ESC Infrastructure is a asynchronous, messaging-based distributed application that incorporates a standards compliant implementation of *Web Services Security* (WS-Security) to enable secure communications across the Internet.

WS-Security is a formally defined is an extension to the *Simple Object Access Protocol* (SOAP) that includes procedures and software protocols for securing Web services. The WS-Security specification describes SOAP messaging enhancements that provide integrity, confidentiality, and mutual authentication for secure data transactions. The WS- Security protocol was originally developed by IBM, Microsoft, and VeriSign and has become a widely adopted open software standard.

WS-Security provides end-to-end transaction security by incorporating security features directly within messages. It specifies how Web services may offer integrity and confidentiality, how digital signatures may be attached and encrypted data embedded within messages. The WS-Security specification provides three mechanisms for securing Web services at the message level: *authentication*, *integrity* and *confidentiality*.

- **Authentication** uses a *security token* to validate users and determine whether a client may access a web service. Clients can be end users, machines, applications, or other web services. Without authentication, an attacker can use spoofing techniques to send a modified message to the service provider.
- **Integrity** uses message signing to ensure that message data is not changed, altered, or lost. Integrity uses *XML digital signatures* on the contents of messages. Without integrity, an attacker can use tampering techniques to intercept a message between the client and server and then modify it.
- **Confidentiality** uses *message encryption* to ensure that only unauthorized parties with proper access may read message information. Without confidentiality, an attacker can use

eavesdropping techniques to intercept a message and read the contained information.

Key Bridge WS-Security implementations provide robust, standards compliant and proven message security solution that meets the most demanding processing and threat environments.

7.3 Software Security

The Java™ platform supports digitally signed application executables, called Java Archive (JAR) files. The ability to sign and verify files is an important part of the Java platform's security architecture. Security is controlled by the security *policy* established and implemented at runtime by the Java virtual machine.

The Java platform enables JAR signing and verification with public and private *keys*, and the X.509 *certificate* that the signer is included in a signed JAR file.

All software incorporated into the ESC Infrastructure will be digitally signed.

This includes the ESC Administration Portal, which will be built with industry standard Java EE and associated enterprise security technologies.

Other applications such as the various servers operating within ESC Service Nodes are expected to be developed as OSGi applications. OSGi is a modular Java operating environment. Securing Java applications running in a OSGi environment is very similar to securing enterprise applications, and for most security frameworks, no additional steps are required. For Java security in enterprise applications, one sets permissions at the application level. For OSGi applications, one may also set security permissions at the bundle (i.e. the JAR) level.

To the extent that embedded Java software is developed and run in a OSGi environment, those applications will be configured with a bundle-level security permission configuration.

8 Key Bridge ESC Commercialization Strategies

The Key Bridge SAS will operate independently from the Key Bridge ESC.

Key Bridge intends to offer commercial ESC services to our own and to other FCC-designated and certified SAS administrator on a non-discriminatory basis. ESC services will be offered through a technologically neutral, standardized peering service.

Current rules entitle a SAS operator to charge CBRS users a reasonable fee for service[28]. Those same rules are silent on a ESC operator's ability to recoup expenses. If anything however, this proposal should illustrate some of the complexity, scale, scope and expense to develop, deploy and operate a ESC Infrastructure.

The 3.5 GHz ecosystem is emergent and still evolving rapidly, as are various underlying commercialization strategies for any fee recovery. Key Bridge does not expect to deploy or to operate a 3.5 GHz ESC as a speculative venture. Rather, Key Bridge intends to operate and to incrementally deploy ESC infrastructure and sensor coverage based upon market demand.

Here we present current options for commercialization that Key Bridge may pursue and their concomitant fee collection processes.

Note that the following descriptions are prospective and Key Bridge may pursue other commercial strategies, possibly to the exclusion of the strategies described here. KEY BRIDGE DOES NOT COMMIT AT THIS TIME TO ANY PARTICULAR COMMERCIAL STRATEGY, DEPLOYMENT, INVESTMENT, FEE STRUCTURES, MARKETING PLAN, ETC.

[28] §96.65(a) “An SAS Administrator may charge … a reasonable fee....”

8.1 Neutral SAS API Services.

Key Bridge expects to support our and other 3.5 GHz Spectrum Access Systems with ESC Infrastructure peering services through neutral SAS to ESC data exchange using the *SAS Gateway Protocol*. The Key Bridge SAS Gateway Protocol is, at present, a proprietary application peering protocol that includes mechanisms to support cryptographically secure message exchange for both SAS to SAS and SAS to ESC peering.

Using the SAS Gateway Protocol, Any FCC-certified SAS administrator may receive ESC services from the Key Bridge ESC by establishing a peering relationship and registering their SAS with the ESC. This concept is shown in Illustration 32 where three client SAS instances each receive spectrum sensing services from the neutral Key Bridge ESC Infrastructure.

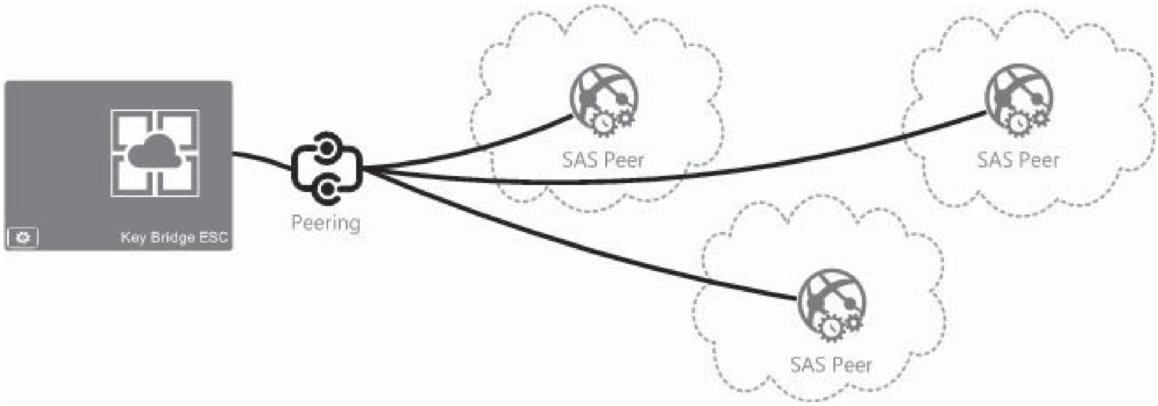


Illustration 32: ESC Infrastructure provides neutral spectrum sensing services.

ESC Infrastructure peering services may be offered on a market-by-market subscription basis and will enable SAS operators to offer spectrum administration services in regions where ESC coverage is required.

8.2 Spectrum Data Reporting.

Key Bridge ESC Sensor Nodes are expected to have sensing capabilities well beyond the 3.5 GHz band. For example, ESC Sensor Nodes presently under development have an effective tuning range and are capable to perform signal detection, identification and classification from 680 to 4,000 MHz. An example scan is shown in Illustration 33.[29]

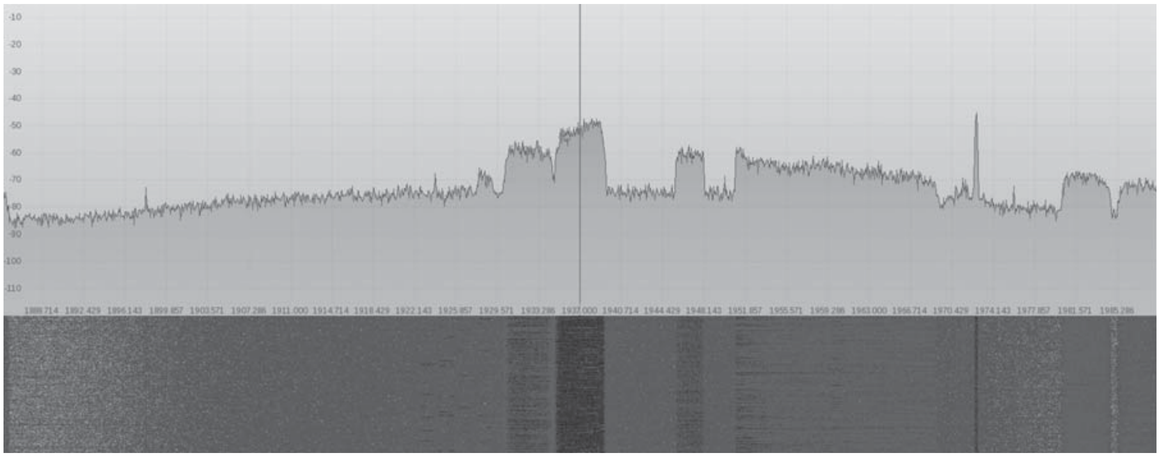


Illustration 33: ESC Sensor Node sample scan from 1,880 to 1,990 MHz.

Once installed the Key Bridge ESC Infrastructure may also be used for wide-area, wide-band spectrum inquiries and study for other spectrum exclusive of the 3.5 GHz band, including:

- Spectrum occupancy, utilization, monitoring and inventory
- Signal search, detection and transmitter identification
- Interference and carrier intrusion detection and resolution
- Continuous spectrum and carrier performance monitoring
- Long-term spectrum characterization and noise floor measurements
- Emitter geolocation

[29] Reproduced with Permission, Courtesy of Cognitive Systems Corp.

8.3 Mapping and Visualization

Key Bridge has experience incorporating spectrum sensor data with our spectrum mapping technologies to enable quick and detailed visual inspection of spectrum environments. This ability combines predicted coverage models with empirical measurement and presents a highly accurate digital representation of real-world spectrum environments.

Key Bridge expects to make available various spectrum mapping technologies that users may exploit for rapid, detailed visual inspection of CBSD spectrum environments and to integrate empirical measurements from the ESC into these mapping services.

Key Bridge already provides spectrum mapping services and capabilities through our commercial API services, and we expect to make these services available to SAS and ESC users through web service and a software developer kit to assist with network planning, device coexistence, and interference avoidance and mediation. An example spectrum coverage map is shown in Illustration 34.[30]

Signal Strength (dBm)
-80
-60
-40
-20
0
© Mapbox © OpenStreetMap Improve this map

Illustration 34: Spectrum situational awareness is enhanced by empirical measurement.

The purpose of generating and using radio coverage maps is to better understand how a transmitter signal may propagate over a geographic region, or correspondingly what limitations on use a receiver may require across a geographic region. In this regard, radio mapping typically need not capture the fine nuances of different propagation model strategies, but instead focus on trending characteristics across an area of operation.

[30] Id.

9 Bibliographic References

Direct Sensing Methodology

Useful and relevant theoretical work in this field includes:

- A. L. Brandao, J. Sydor, and W. Brett, “5 GHz RLAN interference on active meteorological radars,” in IEEE 61st Veh. Tech. Conf., 2005, pp. 1328–1332.
- B.W.Zarikoff, D.Weldon, “Detection of Pulsed Radar in a Time Division Duplexed System”, Vehicular Technology Conference, 2011 IEEE 73rd, pp. 1-5.
- J.Sell, “Measurement Procedures For The Radar Spectrum Engineering Criteria”, U.S. Department Of Commerce, August 1984
- M. Wen and L. Hanwen, “Radar detection for 802.11a systems in 5 GHz band,” in IEEE Int. Conf. on Wireless Commun., Networking and Mobile Computing, 2005, pp. 23–26.
- NTIA Technical Report TR-99-361, 1999, “Technical Characteristics of Radiolocation Systems Operating in the 3.1-3.7 GHz Band and Procedures for Assessing EMC with Fixed Earth Station Receivers”, December 1999
- Ya. D. Shirman And V. N. Golikov, "Fundamentals of the Theory of Detection of Radar Signals and Measurement of their Parameters," U.S. Air Force Foreign Technology Division translation, 1967

Indirect Sensing Methodology

Useful and relevant theoretical work in this field includes:

- B. Lee, Y. Chan, F. Chan, H.-J. Du, and F. A.Dilkes, “Doppler frequency geolocation of uncooperative radars,” MILCOM 2007. IEEE, Oct. 2007
- D. Koks, "Numerical calculations for passive geolocation scenarios," Australian Defense Science and Technology Organization, DSTO-RR-0319, 2007
- Don Koks, Australian Defence Science and Technology Organisation," Numerical Calculations for Passive Geolocation Scenarios", DSTO–RR–0319
- D. Torrieri, “Statistical theory of passive location systems,” Aerospace and Electronic Systems, IEEE Transactions on, vol. AES-20, no. 2, pp. 183 –198, March 1984
- J. Middour, K. Bynum, C. Huffine, A. D’Agostino, C. Chrisman, C. Ellis, and R. Nichols, “Method and apparatus for passively locating radar emissions from rotating transmitters,” U.S. Patent US 7,952,523 B2, May 31, 2011.
- J.Warner, J.W.Middour, "Radar Transmitter Geolocation via Novel Observation Technique and Particle Swarm Optimization," IEEE Aerospace Conference Proceedings, February 2012

Cooperative Sensing Methodology

Examples of interesting and promising theoretical work in this field includes:

- A. Singh, M.R.Bhatnagar, R.K.Mallik, "Cooperative spectrum sensing in multiple antenna based cognitive radio network using an improved energy detector," IEEE Commun. Lett. 2012, 16, 64–67.
- B.F.Lo, I.F.Akyildiz, "Reinforcement learning for cooperative sensing gain in cognitive radio ad hoc networks," Wireless Networks 2013, 19, 1237–1250.
- J.Oksanen, J.Lundén, V.Koivunen, "Reinforcement learning based sensing policy optimization for energy efficient cognitive radio networks," Neurocomputing 2012, 80, 102–110.
- J.Zhao, H.Zheng, G.H.Yang, "Distributed coordination in dynamic spectrum allocation networks," Proceedings of the 2005 First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005, Baltimore, MD, USA, 8–11 November 2005;
- K.L.A.Yau, P.Komisarczuk, P.D.Teal, "Cognitive radio-based wireless sensor networks: Conceptual design and open issues," Proceedings of the IEEE 34th Conference on Local Computer Networks, Zurich, Switzerland, 20–23 October 2009; pp. 955–962.
- K.Hareesh, P.Singh, "An Energy Efficient Hybrid Co-Operative Spectrum Sensing Technique For CRSN," Proceedings of the International Multi Conference on Automation, Computing, Control, Communication and Compressed Sensing (iMac4s-2013), Kottayam, Kerala, 21–23 March 2013; pp. 438–442.
- M. Maida, J. Najim, P. Bianchi, and M. Debbah, “Performance analysis of some eigen-based hypothesis tests for collaborative sensing,” in Proc. IEEE Workshop Datatistical Signal Process., Cardiff, U.K.,2009, pp. 5–8.
- M.Ozger, O.B.Akan, "Event-driven spectrum-aware clustering in cognitive radio sensor networks," Proceedings of the IEEE 2013 INFOCOM, Turin, Italy, 14–19 April 2013; pp. 1483–1491.
- N.Nguyen-Thanh, I.Koo, "A cluster-based selective cooperative spectrum sensing scheme in cognitive radio," EURASIP J. Wirel. Commun. Netw. 2013, 2013, 1–9.
- O.Akan, O.Karli, O.Ergul, "Cognitive radio sensor networks," IEEE Netw. 2009, 23, 34–40. pp. 259–268.
- S.Maleki, A.Pandharipande, G.Leus, "Energy-efficient spectrum sensing for cognitive sensor networks," Proceedings of the IEEE 35th Annual Conference on Industrial Electronics, IECON’09, Porto, Portugal, 3–5 November 2009; pp. 2642–2646.

10 Appendix: The AN/SPN-43 Air Surveillance Radar

ITU allocations for the 3.5 GHz band vary internationally They are identified for IMT in much of Region 1 (EMEA) and 8 areas within Region 3 (Asia/Oceania). In Region 2 (including the US) the band has a Primary allocation for Fixed, Fixed Satellite and Mobile services and has a Secondary allocation for Radio Location Services (RLS). On a US national basis, the 3.5 to 3.65 GHz band is historically allocated to RLS and the ground-based Aeronautical Radio Navigation Service (ARNS) on a primary basis for federal use and on a secondary basis to federal non-military RLS usage. The 3.60 to 3.65 GHz band was additionally allocated to Fixed Satellite Service (FSS) earth stations.

Of the incumbent uses and users presently only the DoD radars are non-informing, and of these the primary non-informing incumbent user is shipborne Navy radar; specifically the AN/SPN-43, an image of which is shown in Illustration 35.[31]

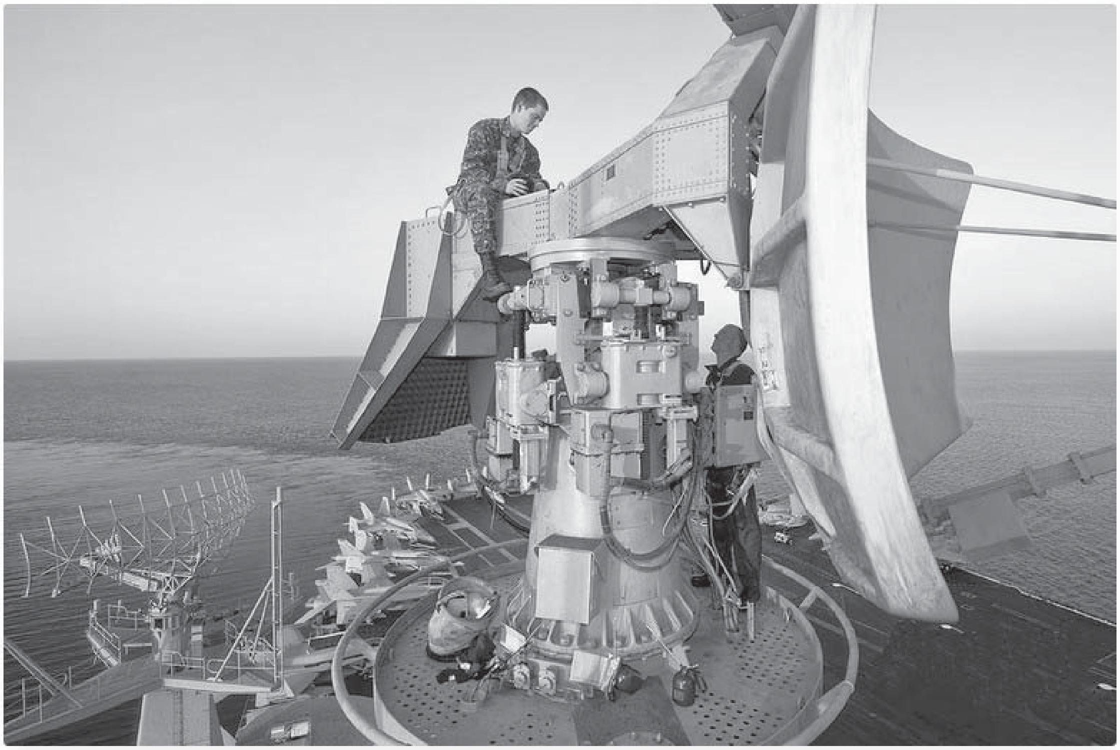


Illustration 35: SPN-43 radar maintenance aboard the USS John C. Stennis.

The AN/SPN-43 is a air traffic control radar used on medium and large aircraft carriers and is the Navy's marshalling air traffic control (ATC) radar system used on all aircraft carriers and amphibious assault ships for vectoring aircraft into final approach. AN/SPN-43 radar systems are mobile shipborne radar systems (primarily installed on U.S. Navy Aircraft Carriers), which can

[31] U.S. Navy photo by Mass Communication Specialist 3rd Class Will Tyndall/Released

be located in all U.S. littoral waters and navigable rivers.

The AN/SPN-43C is a two-dimensional, air traffic control, air-surveillance radar system that provides for simultaneous control and identification of aircraft within a ship's area of responsibility. The AN/SPN-43 provides azimuth and range information from 50 miles to a minimum range of 250 yards at altitudes from radar horizon to 30,000 feet.

The AN/SPN-43C is a coherent on receive radar system with a pulsed magnetron transmitter. The system utilizes a rotating reflector cosecant squared (CSC2) antenna. In a pulsed radar the system radar alternates between transmit and receive modes. This strategy eliminates problems involving the transmitter interfering with the receiver and simplifies range measurement.

AN/SPN-43 Technical Parameters

The AN/SPN-43 air marshaling radar system operates in a 150 MHz band from 3.5 to 3.65 GHz (also reported as 3.59 to 3.7 GHz). SPN-43 transmits high-power pulses through a high-gain antenna that spins azimuthally at a constant rate. AN/SPN-43 system design parameters are listed below in Table 3.[32]

Tuning Range	3.5 - 3.65 GHz [33]
Pulse Generation Method	Magnetron
Pulse Interval	889 (±20) μs
Pulse Width	0.9 (±0.15) μs
Power	850 (±150) kW [34,35]
Emission Designator	P0N [36]
Pulse Repetition Rate	1.125 kHz
Duty Cycle	0.001
Transmitter 3-dB Bandwidth	1.6, 4.0, 16.6 MHz [37]

Table 3: AN/SPN-43 Transmitter Parameters.

The AN/SPN-43 radar uses a mechanically rotating reflector type antenna with an azimuth beam width of 1.5 degree and fan beam in elevation from 5.8 to 45 degree with a main beam gain of 32

[32] Department of Defense, “Military Standardization Handbook,” MIL-HDBK-162B, Dec. 1973.

[33] Department of Defense, AN/SPN-43 Radiation Safety Report. The tuning range is noted as 3.59 - 3.70 GHz.

[34] Radiation Safety Report. Power output is noted at 860 W average, 850 kW PEP.

dBi. The nominal antenna height is 46 meters above the ships water line.[38] System antenna details are listed below in Table 4.

Antenna Type	Reflector
Polarization	Horizontal or circular, switchable
Gain (boresight)	32 dBi
Rotation Period	4 second
Beam width (degree)	4.4 Horizontal / 1.75 Vertical
Notional Antenna Height above waterline	46 meter
Horizontal Scan Type	Rotating
Horizontal Scan Rate	90 (deg./sec)

Table 4: 4.2.2 AN/SPN-43 Antenna Parameters.

AN/SPN-43 Radar Operations

Operational areas of these shipboard radars include both littoral regions and the high seas. These radars typically are operated on a 24-hour schedule. In addition to being located on shipboard platforms, there are fixed installations of these shipboard radars located on land that are used for training and testing. Also, routine maintenance and testing operations require that these radars be activated occasionally in certain ports.

[35] NTIA Technical Report TR-99-361, 1999, “Technical Characteristics of Radiolocation Systems Operating in the 3.1-3.7 GHz Band and Procedures for Assessing EMC with Fixed Earth Station Receivers”, December 1999. (NTIA TR-99-661), Table 6 identifies peak transmit power into Antenna for “Radar A” at 1 MW.

[36] The emission designator “P0N” decodes as P: Sequence of unmodulated pulses, 0: No modulating signal, N: No information transmitted.

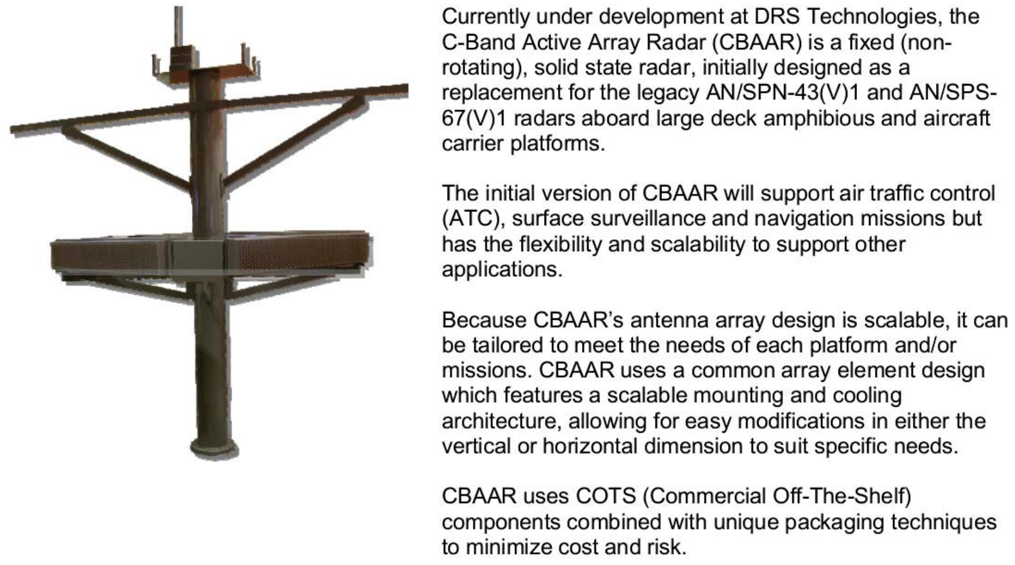
[37] Various sources identify different transmit bandwidth; each is noted.

[38] NTIA TR-99-361 at 4.1.2 *Shipboard Radar Antennas*

AN/SPN-43 Replacement System

In 2012 the Naval Air Systems Command (NAVAIR) issued a public notice seeking a replacement for the AN/SPN-43C Air Surveillance Radar (ASR) in order to resolve ongoing obsolescence issues and radar signal processing deficiencies. In the notice NAVAIR indicated tentatively plans to conduct a full and open competition for the AN/SPN-43C ASR Replacement in the FY-14/early FY-15 time frame in anticipation of award of an engineering and manufacturing development contract by 30 June 2015.[39]

From 2010 to 2012 DRS Technologies advertised a C-Band Active Array Radar (CBAAR): a fixed (non-rotating), solid state radar, initially designed as a replacement for the legacy AN/SPN-43(V)1 and AN/SPS-67(V)1 radars aboard large deck amphibious and aircraft carrier platforms.[40] A media advisory for this program to design, develop and build a solid state, active element, phased array antenna subsystem is shown in Illustration 22.[41]



Currently under development at DRS Technologies, the C-Band Active Array Radar (CBAAR) is a fixed (non-rotating), solid state radar, initially designed as a replacement for the legacy AN/SPN-43(V)1 and AN/SPS-67(V)1 radars aboard large deck amphibious and aircraft carrier platforms.

The initial version of CBAAR will support air traffic control (ATC), surface surveillance and navigation missions but has the flexibility and scalability to support other applications.

Because CBAAR's antenna array design is scalable, it can be tailored to meet the needs of each platform and/or missions. CBAAR uses a common array element design which features a scalable mounting and cooling architecture, allowing for easy modifications in either the vertical or horizontal dimension to suit specific needs.

CBAAR uses COTS (Commercial Off-The-Shelf) components combined with unique packaging techniques to minimize cost and risk.

Illustration 36: DRS CBAAR media advisory excerpt.

[39] FBO.gov Solicitation Number: N0001912R0037 posted February 13, 2012

[40] See http://www.drs.com/Products/C3A/CBAAR.aspx, retrieved February 2015.

[41] Excerpted DRS CBAAR media advisory, released May 5, 2010.